PERSONAL AUTHENTICATING METHOD AND RECORDING MEDIUM RECORDING PERSONAL AUTHENTICATION PROGRAM

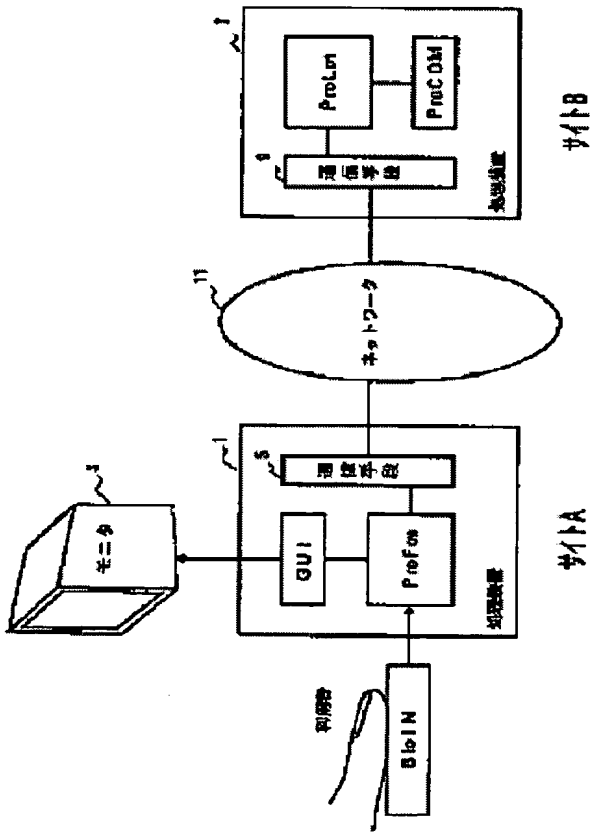
Patent number: JP2001052182
Publication date: 2001-02-23

Inventor: TOMONO AKIRA; KIMURA YOSHIMASA; WAKAHARA TORU; TONAMI MASAFUMI; HORIOKA TSUTOMU; YAMANAKA KIYOSHI; TANAKA KIYOTO; KOMATSU NAOHISA
Applicant: NIPPON TELEGRAPH & TELEPHONE

Classification:
- international: G06T7/00; G06F15/00
- european:
Application number: JP19990229458 19990813
Priority number(s): JP19990229458 19990813

Abstract of **JP2001052182**

PROBLEM TO BE SOLVED: To provide a convinient authentication environment in which any security hole does not exist, a service providing side can check an authentication system and authentication algorithm is easily updated. SOLUTION: In the system connecting a user side terminal 1 and a center side device 7 through a network 11, when performing personal authentication by using human body information, the user side terminal 1 extracts features from the human body information and transmits data showing the features to the center side device 7 and the center side device 7 performs authentication by using the data and previously registered data. In this case, a program for feature extracting processing in the user side terminal is enciphered and transmitted to the user side terminal by the center side device. Besides, the data showing the features are scrambled and transmitted to the center side device by the user side terminal. As human body information, a fingerprint or handwriting can be used.



(19)日本国特許庁（ＪＰ）　(12)公開特許公報（A）　(11)特許出願公開番号
特開2001－52182
（Ｐ２００１－５２１８２Ａ）
(43)公開日　平成13年２月23日(2001.2.23)

(51)Int.Cl.[7]	識別記号	ＦＩ			テーマコード（参考）
G06T 7/00		G06F 15/62	465	A	5B043
G06F 15/00	330	15/00	330	F	5B085
		15/62	460		
			465	P	

審査請求　未請求　請求項の数19　ＯＬ　（全23頁）

(21)出願番号　特願平11－229458

(22)出願日　平成11年８月13日(1999.8.13)

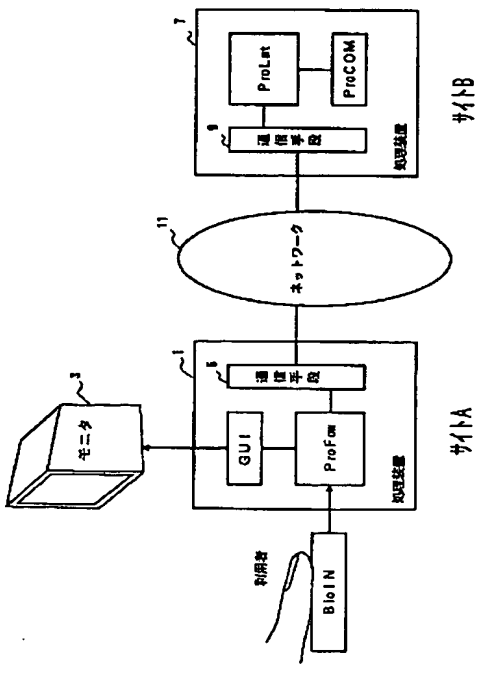
(71)出願人　000004226
日本電信電話株式会社
東京都千代田区大手町二丁目３番１号
(72)発明者　伴野　明
東京都千代田区大手町二丁目３番１号　日本電信電話株式会社内
(72)発明者　木村　義政
東京都千代田区大手町二丁目３番１号　日本電信電話株式会社内
(74)代理人　100070150
弁理士　伊東　忠彦

最終頁に続く

(54)【発明の名称】個人認証方法及び個人認証プログラムを記録した記録媒体

(57)【要約】
【課題】　セキュリティーホールがなく、サービス提供側で認証制度をチェックでき、更に、認証アルゴリズムの更新が容易な使い良い認証環境を提供する。
【解決手段】　利用者側端末とセンタ側装置がネットワークを介して接続されたシステムにおいて、人体情報を用いて個人認証を行うに際し、利用者側端末が人体情報から特徴の抽出を行い、該特徴を示すデータをセンタ側装置に送信し、センタ側装置が前記データと予め登録した登録データを用いて認証を行う。ここで、センタ側装置は利用者側端末における特徴抽出処理のためのプログラムを暗号化して利用者側端末に送信する。また、利用者側端末は特徴を示すデータにスクランブルを掛けてセンタ側装置に送信する。人体情報としては指紋、筆跡等を使用することができる。

本発明における個人認証システムの基本構成を示す図



1

【特許請求の範囲】

【請求項１】　利用者側端末とセンタ側装置がネットワークを介して接続されたシステムにおいて、人体情報を用いて個人認証を行う個人認証方法であって、

該個人認証を行う処理手段は、少なくとも１組の前工程と後工程に分割されており、該前工程と該後工程の境界は適応的に変動可能に構成されており、

該個人認証処理において、該利用者側端末は、

利用者の人体情報入力手段により人体情報を入力し、該人体情報入力手段からの情報を入力として前工程処理手段により前工程処理を行い、該前工程処理手段によって生成される利用者の特徴を示す特徴データをセンタ側装置に伝送し、

該センタ側装置は、

該特徴データを入力として後工程処理手段により後工程処理を行い、該後工程処理手段によって生成される利用者照合データを、判定処理手段を用いて、予め登録されている利用者登録データと比較することによって本人か否かを判定することを特徴とする個人認証方法。

【請求項２】　請求項１に記載の個人認証方法において、

前記少なくとも１組の前工程と前記後工程の境界における特徴データの適応的変動に関して、

前記センタ側装置は、新前工程処理手段と新後工程処理手段とをセットで生成し、該新前工程処理手段を前記利用者側端末に伝送し、

該利用者側端末は、該新前工程処理手段を用いて前回と異なる新特徴データを生成し、

該センタ側装置は、該新特徴データを入力として該新後工程処理手段を用いて利用者照合データを生成することを特徴とする個人認証方法。

【請求項３】　請求項１に記載の個人認証方法において、

前記少なくとも１組の前工程と前記後工程の境界における特徴データの適応的変動に関して、

前記センタ側装置は、前記前工程処理手段にリンクすることによって、前記特徴データにスクランブル等のデータ変換を掛けるデータ変換手段と、前記後工程処理手段にリンクすることによって、該データ変換が掛かった特徴データを入力として、利用者照合データを計算するデータ解読計算手段とをセットで生成するとともに、該データ変換手段を前記利用者側端末に伝送し、

該利用者側端末は、該データ変換手段を該前工程処理手段にリンクして、前回と異なる新特徴データを生成し、

該センタ側装置は、該新特徴データを入力として、該後工程処理手段に該データ解読計算手段をリンクした処理手段を作用させ、利用者照合データを生成することを特徴とする個人認証方法。

【請求項４】　請求項１に記載の個人認証方法において、

2

前記利用者登録データの保管に関して、

前記センタ側装置は、該利用者登録データの写像変換等の暗号化手段と写像解読等の暗号解読手段をセットで用意し、該暗号化手段を用いて、該利用者登録データに写像変換等を施した暗号化データを利用者側端末に伝送し、該暗号化データが正常に伝送されたことを確認した後、該利用者登録データをセンタ側記録媒体から消去し、

該利用者側端末は、該センタ側装置から伝送された該暗号化された利用者登録データを記録媒体に記録し、

利用者登録データの個人認証時の利用に関して、

該利用者側端末は、該センタ側装置に該暗号化された利用者登録データを伝送し、

該センタ側装置は、該写像解読等の暗号解読手段を用いて該写像変換等の暗号化データを解読し、利用者登録データを得た後、前記判定処理手段を用いて、前記利用者照合データと比較することを特徴とする個人認証方法。

【請求項５】　請求項１に記載の個人認証方法において、

前記利用者登録データの保管に関して、

前記利用者側端末は、該利用者登録データの写像変換等の暗号化手段と写像解読等の暗号解読手段をセットで用意し、該暗号化手段を前記センタ側装置に伝送し、

該センタ側装置は、該暗号化手段を用い、該利用者登録データに写像変換等を施した暗号化データを保管するとともに、該利用者登録データを消去する手段を有し、

該利用者登録データの個人認証時の利用に関して、

該利用者側端末は、該センタ側装置に該暗号解読手段を伝送し、

該センタ側装置は、該暗号解読手段を用いて該暗号化された利用者登録データを解読し、利用者登録データを得た後、前記判定処理手段を用いて、前記利用者照合データと比較することを特徴とする個人認証方法。

【請求項６】　請求項５に記載の個人認証方法において、

前記写像変換等の暗号化手段と前記写像解読等の暗号解読手段の前記セットは、必要に応じて更新できるように、プログラムとして記録されていることを特徴とする個人認証方法。

【請求項７】　請求項１に記載の個人認証方法において、

前記センタ側装置から前記利用者側端末への各種処理手段の伝送及び該利用者側端末から該センタ側装置への利用者の特徴を示す特徴データの伝送に関して、

該センタ側装置は、該利用者側端末に、該利用者側端末の公開鍵を用いて、前記前工程処理手段を伝送し、

該利用者側端末は、秘密鍵を用いて該前工程処理手段を取り出し、該前工程処理手段を作動させて、該特徴データを計算し、該秘密鍵を用いて、該特徴データを暗号化して該センタ側装置に伝送し、

該センタ側装置は、該利用者側端末の公開鍵を用いて、該特徴データを取り出し、前記後工程処理を実施することを特徴とする個人認証方法。

【請求項８】　請求項７に記載の個人認証方法において、

前記利用者側端末は、利用者のパスワードを鍵として、秘密鍵を該利用者側端末のフォルダに蓄積管理し、

該利用者が、パスワードを入力することで、秘密鍵を利用可能にすること特徴とする個人認証方法。

【請求項９】　請求項１に記載の個人認証方法において、

前記利用者の人体情報を入力する人体情報入力手段は、カード型の指紋入力装置であって、指紋画像を蓄積して、前記利用者側端末に該画像を伝送する機能を有し、

該利用者側端末が保有する前記前工程処理手段は、特徴要素公開プログラムであって、該プログラムにより計算される利用者特徴要素は、指紋の隆線方向場ベクトルであり、

前記センタ側装置が保有する前記後工程処理手段は、認証データ生成秘密プログラムであり、該プログラムにより計算される利用者登録データ、および、利用者照合データは、数値変換した多次元ベクトルであること特徴とする個人認証方法。

【請求項１０】　請求項１に記載の個人認証方法において、

前記個人認証を行う処理手段の少なくとも１組みの前工程と後工程の分割に関して、

各処理手段は複数ｎ（ｎは自然数）組に分割されており、

前記利用者側端末は、第１番目の前工程結果を前記センタ側装置に送信し、

該センタ側装置は、該処理結果を入力として第１番目の後工程を実施し、該結果を該利用者側端末に伝送し、

該利用者側端末は、該結果を入力として第ｎ番目の前工程を実施し、該結果を該センタ側装置に送信し、

該センタ側装置は、該結果を入力として第ｎ番目の後工程を実施し、利用者照合データを計算することを特徴とする個人認証方法。

【請求項１１】　利用者側端末とセンタ側装置がネットワークを介して接続された、人体情報を用いて個人認証を行う個人認証処理システムにおいて、コンピュータを該個人認証処理を行う該センタ側装置として機能させる個人認証プログラムを記録した記録媒体であって、該個人認証処理を行う手段は、前工程と後工程に分割されており、該前工程と該後工程の境界は適応的に変動可能に構成されており、該利用者側端末は該前工程処理を行う前工程処理手段を有し、

該個人認証プログラムは、

該利用者側端末が該前工程処理により生成した人体情報の特徴データを入力として後工程処理を行う後工程処理手段と、該後工程処理手段によって生成される利用者照合データを、予め登録されている利用者登録データと比較することによって本人か否かを判定する判定処理手段とを有することを特徴とする個人認証プログラムを記録した記録媒体。

【請求項１２】　請求項１１に記載の個人認証プログラムを記録した記録媒体において、前記前工程と前記後工程の境界における特徴データの適応的変動に関して、

該個人認証プログラムは、

新前工程処理手段と、前記利用者側端末における処理のための新後工程処理手段とをセットで生成する手段と、該新前工程処理手段を前記利用者側端末に伝送する手段と、該利用者側端末が該新前工程処理手段を用いて生成した新特徴データを入力として該新後工程処理手段を用いて利用者照合データを生成する手段とを有することを特徴とする個人認証プログラムを記録した記録媒体。

【請求項１３】　請求項１１に記載の個人認証プログラムを記録した記録媒体において、前記前工程と前記後工程の境界における特徴データの適応的変動に関して、

該個人認証プログラムは、

前記前工程処理手段にリンクすることによって、前記特徴データにスクランブルを掛けるスクランブル手段と、前記後工程処理手段にリンクすることによって、該スクランブルが掛かった特徴データを入力として、利用者照合データを計算する計算手段とをセットで生成する手段と、該スクランブル手段を前記利用者側端末に伝送する手段と、

該利用者側端末が該スクランブル手段を用いて生成した該新特徴データを入力として、該後工程処理手段に該計算手段をリンクした処理手段を作用させ、利用者照合データを生成する手段とを有することを特徴とする個人認証プログラムを記録した記録媒体。

【請求項１４】　請求項１１に記載の個人認証個人認証プログラムを記録した記録媒体において、前記利用者登録データの保管に関して、

該個人認証プログラムは、

該利用者登録データの写像変換手段と写像解読手段をセットで用意する手段と、該写像変換手段を用いて、該利用者登録データに写像変換を施した写像変換データを利用者側端末に伝送する手段と、該写像変換データが正常に伝送されたことを確認した後、該利用者登録データをセンタ側記録媒体から消去する手段と、

利用者登録データの個人認証時の利用の際に、該写像解読手段を用いて該利用者側端末が伝送した該写像変換データを解読する手段と、解読により利用者登録データを得た後、前記判定処理手段を用いて、前記利用者照合データと該利用者登録データを比較する手段を有することを特徴とする個人認証プログラムを記録した記録媒体。

【請求項１５】　請求項１１に記載の個人認証プログラムを記録した記録媒体において、前記人体情報は指紋で

あり、前記利用者側端末が保有する前記前工程処理手段は、特徴要素公開プログラムであって、該プログラムにより計算される前記特徴データは、指紋の隆線方向場ベクトルであり、
前記後工程処理手段は、認証データ生成秘密プログラムであり、該プログラムにより計算される利用者登録データ、および、利用者照合データは、数値変換した多次元ベクトルであること特徴とする個人認証プログラムを記録した記録媒体。

【請求項１６】　利用者側端末とセンタ側装置がネットワークを介して接続された、人体情報を用いて個人認証を行う個人認証処理システムにおいて、コンピュータを該個人認証処理を行う該利用者側端末として機能させる個人認証プログラムを記録した記録媒体であって、該個人認証処理を行う手段は、前工程と後工程に分割され、該前工程と該後工程の境界は適応的に変動可能に構成されており、
該個人認証プログラムは、該前工程処理を行う前工程処理手段を有し、
該前工程処理手段は利用者の人体情報を入力する人体情報入力手段からの人体情報を入力として前工程処理を行い、利用者の特徴を示す特徴データを生成し、該特徴データを該センタ側装置に伝送し、該センタ側装置では該特徴データ及び利用者登録データを用いて本人か否かを判定することを特徴とする個人認証プログラムを記録した記録媒体。

【請求項１７】　請求項１６に記載の個人認証プログラムを記録した記録媒体において、前記前工程と前記後工程の境界における特徴データの適応的変動に関して、
該個人認証プログラムは、前記センタ側装置から伝送された新前工程処理手段を用いて前回と異なる新特徴データを生成する手段を有することを特徴とする個人認証プログラムを記録した記録媒体。

【請求項１８】　請求項１６に記載の個人認証プログラムを記録した記録媒体において、前記利用者登録データの保管に関して、
該個人認証プログラムは、該利用者登録データの写像変換手段と写像解読手段をセットで用意し、該写像変換手段を前記センタ側装置に伝送する手段を有し、
該センタ側装置は、該写像変換手段を用い、該利用者登録データに写像変換を施した写像変換データを保管するとともに、該利用者登録データを消去し、
該個人認証プログラムは更に、該利用者登録データの個人認証時の利用に際し、該センタ側装置に該写像解読手段を伝送し、該センタ側装置は、該写像解読手段を用いて該写像変換データを解読することを特徴とする個人認証プログラムを記録した記録媒体。

【請求項１９】　請求項１６に記載の個人認証プログラムを記録した記録媒体において、前記人体情報を入力する人体情報入力手段は、カード型の指紋入力装置であって、指紋画像を蓄積して、前記利用者側端末に該画像を伝送する機能を有し、
前記前工程処理手段は、特徴要素公開プログラムであって、該プログラムにより計算される前記特徴データは、指紋の隆線方向場ベクトルであることを特徴とする個人認証プログラムを記録した記録媒体。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、個人認証方法及びその装置に関し、特に、センサから得られた身体的特徴情報を用いて認証を行う方法及びその装置に関する。

【０００２】

【従来の技術】従来の個人認証方法を説明するにあたり、まず、通信ネットワークを介したサービスにおけるセキュリティ確保について説明する。セキュリティ確保の手段として、公開鍵暗号方式(PKI方式；Pablic Key Infrastructure)が従来から良く知られている。図１３、１４は、その方式の概要と問題点を説明した図である。

【０００３】サイトA とサイトB との間の通信において、サイトB はサービスを提供する側、具体的には、銀行、信販会社、コンテンツ提供会社などである。サイトA はそのサービスを受ける側、具体的には、銀行の預金自動支払い機、信販加入店端末、個人端末などである。ここで、サービスを提供する側は、サイトA に居る利用者が本人であるかどうかを確認する必要がある。

【０００４】従来の公開鍵暗号方式では、先ず、通信開始に先だって、利用者はサイトB に対して証明書の発行要求を行い、サイトB は証明書を発行する。具体的には、利用者が選択した公開鍵に対して、サイトB はサイトA に居る利用者のために秘密鍵を発行し、例えば郵送で利用者に届ける。通信における処理は次の通りである。

【０００５】利用者は、サイトA から通信の要求として、証明書の公開鍵を送信する（ステップ1）。サイトB は、乱数を生成し（ステップ2）、サイトA に送信する（ステップ3）。利用者は、自分の秘密鍵を利用して、その乱数を暗号化してサイトB に伝送する（ステップ4）。サイトB は、利用者の公開鍵を利用して、暗号を解く（ステップ5）。サイトB は、サイトAに送信した乱数と暗号を解読して得た乱数をチェックして、一致していれば、利用者が本人であると認証する（ステップ6）。

【０００６】この処理では、仮に利用者以外の人が秘密鍵を利用できないのであれば、乱数は必ず利用者から送られたことになるので、サイトB は利用者を認証できることになる。ここで、秘密鍵は桁数が多くなると記憶しにくいため、通常利用者は秘密鍵をサイトA （パソコン等）の記憶装置に蓄えて管理する。しかし、この場合、利用者以外の人が、秘密鍵を見るチャンスが生じかねないと言う問題が発生する。仮に、秘密鍵を見られてしま

えば、第３者が正規の利用者に成りすまして、サービスを受ける脅威が生ずる。

【０００７】そこで、第３者がサイトA の記憶装置にアクセスできないように、例えばパスワードを使用して記憶領域に鍵をかける方法が用いられる。しかし、パスワードは盗用される脅威がある。また、サイトA のシステム管理者などはパスワードを知り得る状況にあるため、同様に盗用の脅威がある。すなわち、公開鍵暗号方式は、サイトB とサイトA の間のセキュリティ対策には優れているものの、利用者とサイトA との間のセキュリティは不十分であり、ここにセキュリティホールが存在する。

【０００８】これを補うために、パスワードの変わりに、指紋などの人体情報を用いた個人認証の試みが始まっている。これまで、検討されている個人認証方法の１つとしてオールインワンカードと呼ばれる指紋認証センサつきカードを用いる方法が知られている。このカードは、薄型のカードの中に指紋入力センサが組み込まれており、利用者がセンサに指を当てるとその画像がカード内の一時記憶装置に蓄えられ、画像処理により特徴抽出が行われる。その特徴は、あらかじめ同様にして当該利用者から採取された指紋特徴と照合され、一致かどうかの判定がなされる。カードからは、その認証結果が出力される。この方法によれば、指紋は個人の身体に備わった特徴であり個人ごとに異なるので、パスワードのように見られたら直ぐに盗用されると言った脅威はなくなる。この方式と従来の公開鍵暗号方式を組み合わせれば、前記セキュリティホールの問題は一見解決されるように見える。

【０００９】

【発明が解決しようとする課題】しかしながら、上記の方法にはいくつかの問題がある。第１の問題はカードとパソコンのインタフェースでの脅威である。すなわち、秘密鍵を蓄積してある領域へのアクセスは、カードから出力される本人として認証したかどうかの１ビット情報によるため、カードとパソコンとの間（インタフェース）で信号が盗取される脅威がある。このインタフェース情報が盗取されれば、第３者が利用者に成りすますことも可能である。

【００１０】第２の問題はパソコンから直接秘密鍵を盗取される脅威である。すなわち、パソコンのシステム管理者など、秘密鍵の蓄積領域にアクセスできる者が存在するため、例えば、これらの者を通じて、秘密鍵が盗取される可能性がある。この点は、パスワードを指紋入力に変えたからと言って解決しない問題である。第３の問題はカード製造会社に依存した認証精度評価の問題である。すなわち、カード内に閉じた認証になるため、認証の信頼性などは、カード製造会社に依存せざるを得ない。しかし、本来的には、サービスを提供する側がサービスのリスクを考慮して認証精度を決定することが望ましい。例えば、銀行の預金自動支払いサービスなどにおいて、預金引き出しの額に応じて、本人認証の精度を制御したい場合も考えられる。高額な引き出しの場合には本人認証の精度を高く、低額な預金引き出しであれば使い勝手を優先するなどである。

【００１１】サービス提供会社としては、認証の信頼性を自社で、あるいは、第３者機関でチェック（評価）したいと考えるケースもあるが、カード内で全て秘密に行われるため精度評価が難しい。つまり、認証のアルゴリズムを評価したり、他のアルゴリズムと比較したりすることが難しいと言う問題がある。第４の問題は端末盗難による中身解読の脅威である。サイトA 側において指紋認証を行う従来方式の場合、第３者によりサイトA の認証装置（端末）が盗難され、認証プログラムが解読され、中身が不正に書き換えらたり、コピーされたりする脅威がある。このような脅威は、現実にカード式公衆電話機やカード式パチンコで発生している。それらの装置は個人認証を目的としたものではないが、カードに料金情報など秘密の情報を書き込み、使用料金処理をしている。同装置が一旦盗難に合い、中の処理が解読されると、偽造カードが大量に発行され、社会問題になることもある。

【００１２】第５の問題は認証アルゴリズムのバージョンアップの問題である。第２、第４の問題とも関連するが、認証アルゴリズムが第３者によって解読され、あるいは同様な認証装置（端末や認証カード）が偽造されたような場合、サービス提供側としては、即座に個人認証の方法を変更したいと考えるが、ソフトウエアの更新をサイトA の各端末に対して実施するのはかなりの労力を必要とする。ましてや、認証装置がカードと言うハードウエアで構成されていれば、認証アルゴリズムの更新はカードそのものを変更しなければならず、利用者に配布したカードを回収して、新しい認証方式のカードを配布するための労力、コストは極めて膨大になる。

【００１３】第６の問題は認証の使い易さの問題である。個人認証方法は、利用者の利便性向上、サービス提供側のサービス性向上の観点から、所定の信頼性が確保されるなら、複数の中から選択できることが望ましい。将来の個人認証システムには、モダリティ選択機能が望まれるが、従来は、そのような融通性を持たせた個人認証方法はなかった。

【００１４】本発明は上記の点に鑑みてなされたものであり。下記の目的を有する。まず、第１の目的は通信環境でセキュリティホールのない利用者の個人認証を実現することである。すなわち、サイトA とサイトB との間の通信環境において、従来の方法では、利用者とサイトA との間にセキュリティーホールが存在したが、本発明では、これをなくし、利用者とサイトB との間で確実な認証を実現する。

【００１５】第２の目的はサービス提供側で認証精度の

チェックを可能とすることである。すなわち、従来のように人体情報による認証処理をサービス提供側から見て閉じた環境、例えば、サイトA 、または、利用者が所有するカード等で実現するのではなく、サービス提供側が評価可能な環境で実現する。第３の目的は認証アルゴリズムの更新を容易にすることである。すなわち、認証アルゴリズムに第３者による解読等の脅威があった場合、あるいは、サービス変更に伴い認証に融通性を待たせたい場合などに、認証アルゴリズムを直ぐに更新できる環境を提供する。

【００１６】第４の目的は認証を使い易くすることである。すなわち、利用者の利便性向上、サービス提供側のサービス性向上の観点から、所定の認証信頼性が確保されると言う前提で、複数の人体情報を選択できるようにする。

【００１７】

【課題を解決するための手段】上記の目的を達成するために、本発明はつぎのように構成される。本発明は、利用者側端末とセンタ側装置がネットワークを介して接続されたシステムにおいて、人体情報を用いて個人認証を行う個人認証方法であって、該個人認証を行う処理手段は、少なくとも１組の前工程と後工程に分割されており、該前工程と該後工程の境界は適応的に変動可能に構成されており、該個人認証処理において、該利用者側端末は、利用者の人体情報入力手段（BioIN ）により人体情報を入力し、該人体情報入力手段（BioIN ）からの情報を入力として前工程処理手段（ProFow）により前工程処理を行い、該前工程処理手段（ProFow）によって生成される利用者の特徴を示す特徴データ（Kaz ）をセンタ側装置に伝送し、該センタ側装置は、該特徴データ（Kaz ）を入力として後工程処理手段（ProLat）により後工程処理を行い、該後工程処理手段（ProLat）によって生成される利用者照合データ（Aki ）を、判定処理手段（ProCOM）を用いて、予め登録されている利用者登録データ（AKI ）と比較することによって本人か否かを判定する。

【００１８】上記の構成において、前記少なくとも１組の前工程と前記後工程の境界における特徴データ（Kaz ）の適応的変動に関して、前記センタ側装置は、新前工程処理手段（新ProFow）と新後工程処理手段（新ProLat）とをセットで生成し、該新前工程処理手段（新ProFow）を前記利用者側端末に伝送し、該利用者側端末は、該新前工程処理手段（新ProFow）を用いて前回と異なる新特徴データ（新Kaz ）を生成し、該センタ側装置は、該新特徴データ（新Kaz ）を入力として該新後工程処理手段（新ProLat）を用いて利用者照合データ（Aki ）を生成することもできる。

【００１９】また、上記の構成において、本発明は、前記少なくとも１組の前工程と前記後工程の境界における特徴データ（Kaz ）の適応的変動に関して、前記センタ側装置は、前記前工程処理手段（ProFow）にリンクすることによって、前記特徴データ（Kaz ）にスクランブル等のデータ変換を掛けるデータ変換手段（SXPro 等）と、前記後工程処理手段（ProLat）にリンクすることによって、該データ変換が掛かった特徴データ（Kaz $^{-1}$）を入力として、利用者照合データ（Aki ）を計算するデータ解読計算手段（SXPro $^{-1}$等）とをセットで生成するとともに、該データ変換手段（SXPro 等）を前記利用者側端末に伝送し、該利用者側端末は、該データ変換手段（SXPro 等）を該前工程処理手段（ProFow）にリンクして、前回と異なる新特徴データ（新Kaz ）を生成し、該センタ側装置は、該新特徴データ（新Kaz ）を入力として、該後工程処理手段（ProLat）に該データ解読計算手段（SXPro $^{-1}$等）をリンクした処理手段を作用させ、利用者照合データ（Aki ）を生成するようにしてもよい。

【００２０】また、上記の構成において、前記利用者登録データ（AKI ）の保管に関して、前記センタ側装置は、該利用者登録データ（AKI ）の写像変換等の暗号化手段（ProProj 等）と写像解読等の暗号解読手段（ProProj $^{-1}$等）をセットで用意し、該暗号化手段（ProProj 等）を用いて、該利用者登録データ（AKI ）に写像変換等を施した暗号化データ（AKI $^{-1}$）を利用者側端末に伝送し、該暗号化データ（AKI $^{-1}$等）が正常に伝送されたことを確認した後、該利用者登録データ（AKI ）をセンタ側記録媒体から消去し、該利用者側端末は、該センタ側装置から伝送された該暗号化された利用者登録データ（AKI $^{-1}$等）を記録媒体に記録し、利用者登録データ（AKI ）の個人認証時の利用に関して、該利用者側端末は、該センタ側装置に該暗号化された利用者登録データ（AKI $^{-1}$等）を伝送し、該センタ側装置は、該写像解読等の暗号化手段（ProProj $^{-1}$等）を用いて該写像変換等の暗号化データ（AKI $^{-1}$等）を解読し、利用者登録データ（AKI ）を得た後、前記判定処理手段（ProCOM）を用いて、前記利用者照合データ（Aki ）と比較することとしてもよい。

【００２１】更に、前記利用者登録データ（AKI ）の保管に関して、前記利用者側端末は、該利用者登録データ（AKI ）の写像変換等の暗号化手段（ProProj 等）と写像解読等の暗号解読手段（ProProj $^{-1}$等）をセットで用意し、該暗号化手段（ProProj 等）を前記センタ側装置に伝送し、該センタ側装置は、該暗号化手段（ProProj 等）を用い、該利用者登録データ（AKI ）に写像変換等を施した暗号化データ（AKI $^{-1}$等）を保管するとともに、該利用者登録データ（AKI ）を消去する手段を有し、該利用者登録データ（AKI ）の個人認証時の利用に関して、該利用者側端末は、該センタ側装置に該暗号解読手段（ProProj $^{-1}$等）を伝送し、該センタ側装置は、該暗号解読手段（ProProj $^{-1}$等）を用いて該暗号化された利用者登録データ（AKI $^{-1}$等）を解読し、利用者登録データ（AKI ）を得た後、前記判定処理手段（ProCOM）

を用いて、前記利用者照合データ（Aki ）と比較することもできる。

【００２２】また、上記の構成において、前記写像変換等の暗号化手段（ProProj 等）と前記写像解読等の暗号解読手段（ProProj $^{-1}$等）の前記セットは、必要に応じて更新できるように、プログラムとして記録されている（ProSET）こととしてもよい。また、上記の構成において、前記センタ側装置から前記利用者側端末への各種処理手段の伝送及び該利用者側端末から該センタ側装置への利用者の特徴を示す特徴データ（Kaz ）の伝送に関して、該センタ側装置は、該利用者側端末に、該利用者側端末の公開鍵 Pk(siteA)を用いて、前記前工程処理手段（ProFow）を伝送し、該利用者側端末は、秘密鍵 Sk(siteA)を用いて該前工程処理手段（ProFow）を取り出し、該前工程処理手段（ProFow）を作動させて、該特徴データ（Kaz）を計算し、該秘密鍵 Sk(siteA)を用いて、該特徴データ（Kaz ）を暗号化して該センタ側装置に伝送し、該センタ側装置は、該利用者側端末の公開鍵 Pk(siteA)を用いて、該特徴データ（Kaz ）を取り出し、前記後工程処理を実施することもできる。

【００２３】上記の構成においては、前記利用者側端末は、利用者UAのパスワードPWを鍵として、秘密鍵 Sk(siteA)を該利用者側端末のフォルダに蓄積管理し、該利用者UAが、パスワードPWを入力することで、秘密鍵 Sk(siteA)を利用可能にすることとしてもよい。また、上記の構成において、前記利用者UAの人体情報を入力する人体情報入力手段（BioIN ）は、カード型の指紋入力装置であって、指紋画像を蓄積して、前記利用者側端末に該画像を伝送する機能を有し、該利用者側端末が保有する前記前工程処理手段（ProFow）は、特徴要素公開プログラムであって、該プログラムにより計算される利用者特徴要素Kaz は、指紋の隆線方向場ベクトルであり、前記センタ側装置が保有する前記後工程処理手段（ ProLat ）は、認証データ生成秘密プログラムであり、該プログラムにより計算される利用者登録データ（AKI ）、および、利用者照合データ（Aki ）は、数値変換した多次元ベクトルであることとしてもよい。

【００２４】更に、上記構成において、前記個人認証を行う処理手段の少なくとも１組みの前工程と後工程の分割に関して、各処理手段は複数ｎ（ｎは自然数）組に分割されており、前記利用者側端末は、第１番目の前工程結果を前記センタ側装置に送信し、該センタ側装置は、該処理結果を入力として第１番目の後工程を実施し、該結果を該利用者側端末に伝送し、該利用者側端末は、該結果を入力として第ｎ番目の前工程を実施し、該結果を該センタ側装置に送信し、該センタ側装置は、該結果を入力として第ｎ番目の後工程を実施し、利用者照合データを計算することとしてもよい。

【００２５】上記の通り、本発明によれば、個人認証の工程を端末側の処理とセンタ側の処理とに分け、端末側からは特徴を示すデータを送信することとしているので、人体情報そのものを送信する場合に比較してデータ伝送量を削減でき、また、認証結果を送信する場合より高いセキュリティーを得ることが可能である。また、伝送データを暗号化したり、スクランブルをかけることにより更にセキュリティーを高めることが可能となる。また、サービスの提供側で認証精度のチェックが可能となる。また、登録データを利用者側端末に置くことが可能となり、セキュリティー及び利用者にとっての利便性が更に向上する。

【００２６】また、センタ側装置は最適なプログラムを端末側に送ることが可能となり、認証アルゴリズムを容易に更新することが可能となる。更に、利用者と利用者側端末間のセキュリティーホールがなくなり、確実な認証が可能となる。上記の目的を達成するために、本発明はつぎのように構成することも可能である。

【００２７】本発明は、利用者側端末とセンタ側装置がネットワークを介して接続された、人体情報を用いて個人認証を行う個人認証処理システムにおいて、コンピュータを該個人認証処理を行う該センタ側装置として機能させる個人認証プログラムを記録した記録媒体であって、該個人認証処理を行う手段は、前工程と後工程に分割されており、該前工程と該後工程の境界は適応的に変動可能に構成されており、該利用者側端末は該前工程処理を行う前工程処理手段を有し、該個人認証プログラムは、該利用者側端末が該前工程処理により生成した人体情報の特徴データ（Kaz ）を入力として後工程処理を行う後工程処理手段と、該後工程処理手段によって生成される利用者照合データ（Aki ）を、予め登録されている利用者登録データ（AKI ）と比較することによって本人か否かを判定する判定処理手段（ProCOM）とを有する。

【００２８】上記の構成において、前記前工程と前記後工程の境界における特徴データ（Kaz ）の適応的変動に関して、該個人認証プログラムは、新前工程処理手段（新ProFow）と、前記利用者側端末における処理のための新後工程処理手段（新ProLat）とをセットで生成する手段と、該新前工程処理手段（新ProFow）を前記利用者側端末に伝送する手段と、該利用者側端末が該新前工程処理手段（新ProFow）を用いて生成した新特徴データ（新Kaz ）を入力として該新後工程処理手段（新ProLat）を用いて利用者照合データ（Aki ）を生成する手段とを有することとしてもよい。

【００２９】また、上記の構成において、該個人認証プログラムは、前記前工程処理手段（ProFow）にリンクすることによって、前記特徴データ（Kaz ）にスクランブルを掛けるスクランブル手段（SXPro ）と、前記後工程処理手段（ProLat）にリンクすることによって、該スクランブルが掛かった特徴データ（Kaz $^{-1}$）を入力として、利用者照合データ（Aki ）を計算する計算手段（SX Pro $^{-1}$）とをセットで生成する手段と、該スクランブル

手段（SXPro ）を前記利用者側端末に伝送する手段と、該利用者側端末が該スクランブル手段（SXPro ）を用いて生成した該新特徴データ（新Kaz ）を入力として、該後工程処理手段（ProLat）に該計算手段（SXPro $^{-1}$）をリンクした処理手段を作用させ、利用者照合データ（Aki ）を生成する手段とを有してもよい。

【００３０】また、上記の構成において、前記利用者登録データ（AKI ）の保管に関し、該個人認証プログラムは、該利用者登録データ（AKI ）の写像変換手段（ProProj）と写像解読手段（ProProj $^{-1}$）をセットで用意する手段と、該写像変換手段（ProProj ）を用いて、該利用者登録データ（AKI ）に写像変換を施した写像変換データ（AKI $^{-1}$）を利用者側端末に伝送する手段と、該写像変換データ（AKI $^{-1}$）が正常に伝送されたことを確認した後、該利用者登録データ（AKI ）をセンタ側記録媒体から消去する手段と、利用者登録データ（AKI ）の個人認証時の利用の際に、該写像解読手段（ProProj $^{-1}$）を用いて該利用者側端末が伝送した該写像変換データ（AKI $^{-1}$）を解読する手段と、解読により利用者登録データ（AKI）を得た後、前記判定処理手段（ProCOM）を用いて、前記利用者照合データ（Aki ）と該利用者登録データ（AKI ）を比較する手段を有することも可能である。

【００３１】また、上記の構成において、前記人体情報は指紋であり、前記利用者側端末が保有する前記前工程処理手段（ProFow）は、特徴要素公開プログラムであって、該プログラムにより計算される前記特徴データ（Kaz ）は、指紋の隆線方向場ベクトルであり、前記後工程処理手段（ ProLat ）は、認証データ生成秘密プログラムであり、該プログラムにより計算される利用者登録データ（AKI ）、および、利用者照合データ（Aki ）は、数値変換した多次元ベクトルであることとしてもよい。

【００３２】上記の記録媒体に記録されたプログラムをコンピュータにインストールすることによって、本発明の個人認証方法を実行することができる。上記の目的を達成するために、更に本発明はつぎのように構成することも可能である。本発明は、利用者側端末とセンタ側装置がネットワークを介して接続された、人体情報を用いて個人認証を行う個人認証処理システムにおいて、コンピュータを該個人認証処理を行う該利用者側端末として機能させる個人認証プログラムを記録した記録媒体であって、該個人認証処理を行う手段は、前工程と後工程に分割され、該前工程と該後工程の境界は適応的に変動可能に構成されており、該個人認証プログラムは、該前工程処理を行う前工程処理手段を有し、該前工程処理手段は利用者の人体情報を入力する人体情報入力手段（BioIN ）からの人体情報を入力として前工程処理を行い、利用者の特徴を示す特徴データ（Kaz ）を生成し、該特徴データ（Kaz ）該センタ側装置に伝送し、該センタ側装置では該特徴データ（Kaz ）及び利用者登録データ(AKI)を用いて本人か否かを判定する。

【００３３】上記の構成において、前記前工程と前記後工程の境界における特徴データ（Kaz ）の適応的変動に関して、該個人認証プログラムは、前記センタ側装置から伝送された新前工程処理手段（新ProFow）を用いて前回と異なる新特徴データ（新Kaz ）を生成する手段を有することとしてもよい。また、上記の構成において、前記利用者登録データ（AKI ）の保管に関して、該個人認証プログラムは、該利用者登録データ（AKI ）の写像変換手段（ProProj ）と写像解読手段（ProProj $^{-1}$）をセットで用意し、該写像変換手段（ProProj ）を前記センタ側装置に伝送する手段を有し、該センタ側装置は、該写像変換手段（ProProj ）を用い、該AKI に写像変換を施した写像変換データ（AKI $^{-1}$）を保管するとともに、該利用者登録データ（AKI ）を消去し、該個人認証プログラムは更に、該利用者登録データ（AKI ）の個人認証時の利用に際し、該センタ側装置に該写像解読手段（ProProj $^{-1}$）を伝送し、該センタ側装置は、該写像解読手段（ProProj $^{-1}$）を用いて該写像変換データ（AKI $^{-1}$）を解読することとしてもよい。

【００３４】更に、上記の構成において、前記人体情報を入力する人体情報入力手段（BioIN ）は、カード型の指紋入力装置であって、指紋画像を蓄積して、前記利用者側端末に該画像を伝送する機能を有し、前記前工程処理手段（ProFow）は、特徴要素公開プログラムであって、該プログラムにより計算される前記特徴データ（Kaz ）は、指紋の隆線方向場ベクトルであることとしてもよい。

【００３５】上記の記録媒体に記録されたプログラムをコンピュータにインストールすることによっても、本発明の個人認証方法を実行することができる。本発明の更なる機能、特徴については発明の実施の形態において添付の図面を参照して詳細に説明する。

【００３６】

【発明の実施の形態】次に、本発明の実施例における個人認証システムについて、図面を参照して説明する。図１に本発明の実施の形態における個人認証システムの基本構成を示す。なお、図１は主要な構成要素を示しており、詳細については各実施例中で説明する。

【００３７】本実施の形態において、サイトA には、所定のプログラムに従って処理を実行するパソコン等の処理装置１と、利用者UAの人体情報を入力する手段BioINが備えられている。BioIN はその処理装置に接続されている。また、画面表示を行うためのモニタ３が処理装置１に接続される。その処理装置には特徴要素抽出のための前工程プログラムProFow、モニタ３にバイオデータ取得方法などのガイド情報を示すプログラムGUI 、他の装置と通信を行うための通信手段５が備えられる。なお、BioIN やProFow等は各構成要素を示す記号であり、以下、記号のみでその要素を参照する場合がある。以下で

15

新たに説明する要素についても同様である。

【００３８】さて、BioIN の例としては、指紋入力センサがある。指紋の検出方式としては光学式、静電容量式などがあり、例えば、300x300 画素、8bit階調、500dpi程度の性能を持つ指紋画像が出力される。ProFow、GUIは、サイトB から伝送されても良いし、CD-ROMやフロッピーディスク等に記録し、郵送等されたものをサイトAでインストールしてもよい。

【００３９】サイトB には、所定のプログラムに従って処理を実行するコンピュータ等の処理装置７が備えられる。処理装置７はセンタ側装置、あるいは認証サーバと称してもよい。処理装置７には、サービス提供側サイトA で計算される後述の利用者特徴要素Kaz を入力として、バイオ認証登録データAKI 、または、認証データAki を計算する後工程プログラムProLat、AKI とAki とを比較する認証データ比較プログラムProComが備えられる。また、通信手段９を有し、ネットワーク１１を介してサイトA の処理装置１と通信を行なう。

【００４０】動作の概要は次の通りである。詳細動作については後述する。利用者UAの操作により、サイトA からサイトB に対してサービス要求Req すると、サイトBは、サイトA の画面を通じて、利用者にセンサに指を乗せるように指示する。具体的には、GUI プログラムを作動させると、利用者との対話形式により、センサに置く指の種類、方向などが指示される。その指示通りに、指を乗せると指紋画像が取得できる。サイトＡは特徴要素Kaz を抽出し、サイトＢに伝送する。伝送する方法としては、例えば、サイトA が予め公開鍵暗号方式に基づく公開鍵、秘密鍵を保有しており、秘密鍵を用いて特徴要素Kaz を暗号化して伝送する方法が考えられる。秘密鍵の管理に関しては、サイトA に秘密鍵を保管するフォルダを設け、このフォルダの開閉にパスワードPWを記憶鍵として用いる方法が考えられる。つまり、利用者は、GUI プログラムの指示に従って、センサに指を乗せた後、PWを入力して秘密鍵を取り出し、この秘密鍵を用いてを暗号化して、サイトB に伝送する。

【００４１】サイトB では、暗号化されたKaz を受信すると、公開鍵を用いてこれを解読し、Kaz を得る。次にKaz を入力として、後工程プログラムProLatを作動させ、特徴要素Kaz を入力として認証データAki を計算する。ProLatの処理が済んだデータを利用者の認証が可能になったデータと言う意味で認証データAki と称している。

【００４２】その認証データ Akiは、通信に先だって同様な方法で計算されたバイオ認証登録データAKI と比較する。このプログラムが認証データ比較プログラムProCOMである。ProCOMの具体的な処理例はしきい値処理であり、Aki がAKI と比較して所定のしきい値条件を満たした場合、利用者UAを本人と認証し、満たさなかった場合、認証しない。

16

【００４３】次に、上記の構成要素のうち特徴要素抽出処理を行うProFowの機能についてより詳細に説明する。指紋入力センサからの出力は、パソコン等の処理装置内に取り込まれ、画像処理として、指紋画像のノイズ除去処理、細線化処理などが実施され、特徴要素抽出処理として、小ブロック分割処理、小ブロック内の切断・分岐点検出処理、小ブロック内の隆線ベクトル検出処理などが実施される。ここでは、小ブロック内の切断・分岐点マップ（これはマニューシャと呼ばれる）、あるいは、小ブロック内の隆線ベクトルを利用者の特徴要素Kaz と呼ぶ。

【００４４】Kaz が隆線ベクトルの場合の例を図２に示す。300x300 画素を10x10 画素のブロックに分割すると、小ブロックが30x30 できる。指がセンサの何処に触れるか分からないので、画像を取り込んだ後、先ず、大まかな位置あわせを行う（平行移動と回転）。位置合わせには、ずらしマッチングによる誤差最小法、または、マニューシャ情報のマッチングを用いてもよい。位置合わせの後、各小ブロックについて指紋の隆線を検出し、その方向を例えば、16方向で代表させ4bitで表すと、Kaz は、図３のように、900 次元（各次元4bit）のベクトルになる。

【００４５】この隆線ベクトルは、仮に指の位置を大まかに合わせても、指をセンサに乗せるタイミング、押す圧力、皮膚の弾力性などにより変化する。つまり、ある揺らぎを持って個人毎に異なる特徴を示す。次に、後工程処理プログラムProLatによる認証データAki を求める計算処理について説明する。Kaz からAki を求める計算としては、変数変換、異次元特徴空間への展開が考えられる。

【００４６】まず、変数変換の具体例を以下に説明する。図３のようにして隆線ベクトルが得られたとする。各次元は指紋の方向性を示しているが、離散値である。図４（ａ）は、２本の指紋隆線の和を求めた概念を示したものである。ここで、指紋は明瞭に検出される場合と掠れる場合がある。上側の隆線が掠れて明瞭でない場合、２本の指紋隆線の和は、図４（ｂ）のように、図４（ａ）の場合より右回転の大きなベクトルになる。掠れやすい部分は、個体間で共通なものと、個体内に閉じている場合がある。

【００４７】いずれの場合であっても、その傾向が分かっていれば変換が可能である。具体的には、あるベクトル次元において取るべき方向の偏りが分かっていれば（統計的に求めておけば）この係数を掛け、離散値を変更できる。このような処理は、指紋の大量のデータベースに基づいて処理しなければならず、サイトB のサーバにおいて実施しやすい処理である。

【００４８】次に、異次元特徴空間への展開の具体例を説明する。隆線ベクトルの各次元（または、所定の部分次元列）について、信頼度が異なることがある。指紋が

明確に検出できてその方向も安定している場合はその方向の離散値は高いと言えるが、センサの上記部分小ブロック内に複数の隆線が混入しその線が明瞭でない場合はその方向の離散値の信頼度は低いと言える。

【００４９】従って、このように各ブロック毎に信頼度を求めておき、検出された隆線ベクトルに信頼度を掛けて、照合処理をしても良い。信頼度を掛けた特徴空間は、信頼度を掛けない特徴空間に対して歪んでいるので、一種の異次元特徴空間と言える。更に、センサが複数あり、各センサから異種の特徴が得られる場合、この統合処理も後工程プログラムProLatでおこなう。その詳細は後述する。

【００５０】本発明の個人認証システムにおける一連の処理の中には、「ア；画像入力処理」「イ；雑音除去処理」「ウ；細線化処理」「エ；隆線抽出処理」「オ；隆線ブロック化処理（隆線ベクトル抽出処理）」「カ；隆線の端点・分岐点抽出処理（マニューシャ抽出処理）」「キ；特徴データスクランブル処理」「ク；特徴データスクランブル解読処理」「ケ；特徴データ重み付け処理」「コ；複数特徴統合化処理」「サ；利用者照合データ生成処理」「シ；登録データ照合データ比較判定処理」等がある。本発明においては、「キ」までを前工程、「ク」からを後工程とするのみでなく、「ア、ウ、オ、キ、ケ、サ」を前工程、「イ、エ、カ、ク、コ、シ」を後工程とすることも可能である。また、その他の組み合わせも可能である。適応的に分割可能とはこのような分割も含まれる。

【００５１】続いて、上記個人認証システムの動作を、３つの実施例を取り上げて図を参照して説明する。まず、第１の実施例における通信開始に先立って行われる利用者登録処理について図５のフロー図を用いて説明する。サイトA を利用する利用者UAから証明書発行要求、つまり、公開鍵の証明要求があると（ステップ０－１）、サイトB では、サイトA の秘密鍵を生成し（ステップ１－１）、これら情報を証明書の発行として、サイトA に送る（ステップ２）。ここまでは、従来の公開鍵暗号方式による認証方式と同様である。

【００５２】本発明では、サービスを受けるには、バイオ証明書の発行が必要となる。それは以下のような処理により行われる。サイトA からバイオ証明書発行要求があると、サイトB では、バイオ認証プログラムを生成する。具体的には、GUI 制御プログラムProGUI、特徴要素抽出のための前工程プログラムProFow、認証データ生成のための後工程プログラムProLat、認証データ比較プログラムProCOMを生成する（ステップ１－２）。

【００５３】ProGUIとProFowは、サイトA の公開鍵Pk(siteA) で暗号化されサイトB からサイトA に伝送される（ステップ３）。サイトA では、秘密鍵Sk(siteA) を用いてこれを解読し、ProGUIとProFowを取り出す（ステップ５）。ここで、秘密鍵Sk(siteA) の利用に関しては、パスワードPWを併用してもよい（ステップ４）。ProGUIは、サイトA にインストールされて、利用者UAに画面との対話形式で指紋入力などを指示する（ステップ６）。続いて、ProFowは特徴要素抽出処理を行う（ステップ７）。

【００５４】具体的には、指をセンサに乗せる（ステップ７－１）とセンサは、指紋画像FIN-Ima を取得し（７－２）、サイトA の処理装置に伝送する。次に、特徴要素抽出プログラムProFowを作動し（７－３）、その結果である利用者特徴要素Kaz_0を抽出する（ステップ７－４）。ここで、記号Kaz_0における0 は登録時、つまり初回を意味する。

【００５５】図５には、Kaz_0の具体例として、情報量を示している。生データは300X300 画素で90KByte 、隆線の方向場ベクトルは5KByte、指紋パターンの分岐点、端点等を集めたマニューシャ情報は300Byte 程度であり、これらは全て実施可能である。ここでは主に、Kaz_0の具体例として、隆線の方向場ベクトルを考える。同ベクトルの場合、通常1000次元以上もあるので、指を押す度に変化すると考えられる。なお、特徴要素抽出処理の詳細については後述する。

【００５６】続いて、Kaz_0は、秘密鍵Sk(siteA) で暗号化して、サイトB に伝送される（ステップ８－１）。これは、サイトA の利用者の署名を付けてサイトB に伝送することを意味している。サイトB では、公開鍵Pk(siteA) を用いて、Kaz_0を得る（ステップ８－２）。サイトB は、確実にA から伝送されたことが分かる。次に、認証データ生成のための後工程プログラムProLatを作動し、認証登録データAKI_0を計算する（ステップ１０）。そして、AKI_0は、サイトB において鍵を掛けて保管する（ステップ２０）。

【００５７】続いて、第１の実施例における通信中の処理について図６を用いて説明する。利用者UAからサービス要求があると（ステップ１）、サイトB は、パスワード入力および指紋入力を要求する。以降、利用者登録処理と同様なステップ４～ステップ８－２の処理によって、$Kaz_{\blacksquare}$（m 回目のKaz を意味する）が計算され、暗号化され、サイトB に伝送され、サイトB では、暗号を解読し、$Kaz_{\blacksquare}$を得る。次に、認証データ生成のための後工程プログラムPloLatを作動し、認証データ$Aki_{\blacksquare}$を計算する（ステップ１０）。そして、AKI_0を金庫から取り出し（ステップ１１）、ProComを作動し、$Aki_{\blacksquare}$とAKI_0を比較し、$Aki_{\blacksquare}$がAKI_0の許容範囲であれば認証する（ステップ１２）。

【００５８】ここで、AKI_0の保管に関して、サイトB に保管されることに心理的抵抗感がある場合には、AKI_0をサイトB の秘密鍵で暗号化したデータAKI_0^{-1}を、サイトA の公開鍵で暗号化して、サイトA に伝送し、サイトA では、サイトA の秘密鍵でこれを解き、AKI_0^{-1}をサイトA で保管しても良い。サイトB でAKI_0を利用する際は、

サイトB はサイトA から、AKI_0^{-1}を伝送してもらい、サイトB の秘密鍵で解き、AKI_0を再生して使用してもよい。

【００５９】利用者の本人確認が出来た後は、サイトB は、サイトA の公開鍵Pk(siteA) を用いてコンテンツを暗号化して、サイトA に伝送する（ステップ３０）。また、サイトA では秘密鍵Sk(siteA) を用いて暗号を解き、そのコンテンツを得ることができる（ステップ３１）。次に、第２の実施例について説明する。第２の実施例は、サイトA において、利用者UAの特徴要素Kaz を第三者に盗取されないようにするための発明の実施例であって、サイトA でKaz を計算する過程において、サイトB が保有するスクランブル解読プログラムによってのみ解読できるようなスクランブルをKaz に施す処理を行う。

【００６０】また、サイトB において計算したAKI をサイトB 側の第三者が簡単に読み出せないようにするため、AKI を写像変換してサイトA に伝送し、写像変換されたAKI をサイトA において保管する。ここでの写像変換とは、例えば、ｎ次元の特徴空間があった場合、各次元に乱数等の係数を掛けることで、特徴データを意味不明にする。また、写像解読とは掛けた乱数で割って元に戻すこと等の方法がある。

【００６１】また、暗号化、暗号解読（あるいは復号化）とは、各次元の特徴コードを共通鍵暗号方式、公開鍵暗号方式などで、更に安全に保護することである。第２の実施例における利用者登録処理を図７を用いて説明する。以下、図５と異なる点のみ説明する。図には下二重線で示す。サイトA から、サイトB にバイオ証明書発行要求があると（ステップ０－１）、サイトB は、特徴要素抽出プログラムProFowと共に、ProFowにリンクすることでKaz の順列にスクランブルを掛けるスクランブルプログラムSXPro と、このスクランブルを解読してKaz を復元するスクランブル解読プログラムSXPro $^{-1}$を生成する。更に、認証データ生成プログラムProLatと共に、該ProLatにリンクすることでAKI を簡単に解読できなくする写像変換プログラムProProj と、この写像を解読するプログラムProProj $^{-1}$、および、認証データ比較するプログラムProComを生成する（ステップ１－２）。サイトA には、通信開始に先だって、サイトB から ProFow とSXPro が伝送される。二つのプログラムはリンクされ、スクランブルされたKaz が計算される機能となる。

【００６２】同図（ステップ７）において、利用者が指紋を入力すると、 ProFow とSXProによって、スクランブルされた$Kaz_{0,n}^{-1}$が計算される（ステップ７－５）。ここで、ｎはｎ回目に伝送されるSXPro を示す。ここで、ProFowは、Kaz を計算する指紋認証アルゴリズムに直接関わるプログラムの前半部分なので頻繁に変更することはない。一方、SXPro はKaz のスクランブル機能であって、直接、認証アルゴリズムに係わらないプログラムなので、頻繁に変更する。例えば、認証要求の度に変更しても良い。

【００６３】ステップ８－１において、$Kaz_{0,n}^{-1}$はサイトA の秘密鍵Sk(siteA) で暗号化してサイトB に伝送する。これは、サイトA の利用者UAの署名を付けてサイトB に伝送することを意味し、サイトB は公開鍵Pk(siteA) を用いて解読し、$Kaz_{0,n}^{-1}$を得る（ステップ８－２）。サイトA の公開鍵を用いて解読することで、確実にサイトA から送られたことが分かる。

【００６４】ステップ９において、スクランブル解読プログラムSXPro $_n^{-1}$を用い、利用者特徴要素Kaz_0を復元する。ステップ１０において、認証データ生成プログラム(秘密) ProLatを作動し、認証登録データAKI_0を計算する。ステップ１１において、ｎ回目の写像変換プログラムProProj $_n$ を用いて、AKI_0の写像$AKI_{0,n}^{-1}$を計算する。毎回異なる写像データにするので、サイトA 、 Bのどちらに保管しても偽造が難しい。

【００６５】ここで、ProLatを作動させAKI_0を計算し、この結果をProProj $_n$ の入力として、AkI0,n-1を計算するのではなく、ProLatとProProj $_n$ をリンクして、これにKaz$_0$を入力として、直接に$AKI_{0,n}^{-1}$を計算する方法を用いても良い。ステップ１２において、$AKI_{0,n}^{-1}$をサイトA の公開鍵Pk(siteA) で暗号化し、サイトA に伝送する。公開鍵を用いることで、この暗号化されたデータはサイトA の利用者UA以外の者が解読できないので、確実にサイトA に送ることができる。ステップ１３において、秘密鍵Sk(siteA) で解読して、$AKI_{0,n}^{-1}$を計算し、ステップ１４において、次の図８に示す通信中の処理のために、ｎ をn-1 に置き換えて、$AKI_{0,n-1}^{-1}$をサイトA に保管（蓄積）する。

【００６６】ステップ１５～１７にて、$AKI_{0,n-1}^{-1}$がサイトB からサイトA に確実に伝送されたことを確認した後、サイトB のAKI_0を消去する。このようにすることで、AKI_0はサイトB にも、サイトA にも残らないので、盗取などに対して安全である。次に、第２の実施例における通信中の処理を図８を用いて説明する。以下、図６と異なる部分のみ説明する。

【００６７】ステップ１において、サイトB にサービス要求があると、サイトB は、スクランブルプログラムSXPro $_n$ 、同解読プログラムSXPro $_n^{-1}$、写像変換プログラムProProj $_n$ 、写像解読プログラムProProj $_n^{-1}$を生成する。ステップ７、８において、利用者がm 回目の指を押すと、Kazmが得られ、これにスクランブルを掛け、Kazm-1を得る。これと、前回写像変換された認証登録データ$AKI_{0,n-1}^{-1}$とを公開鍵暗号方式で、サイトB に伝送する。サイトB では、ステップ８－２において、これを解き、Kazm-1と$AKI_{0,n-1}^{-1}$を得る。

【００６８】ステップ１０において、ProLatを用いて、Aki $_n$ を計算し、ステップ１１において、前回用いた写像変換を解読するプログラムProProj $_{n-1}^{-1}$を用い、AK

$I_{0,n}^{-1}$を入力として、AKI_0を計算する。ステップ１２において、ProComを用いて、Aki $_n$ とAKI_0とを比較する。もし、Aki $_n$ がAKI_0の許容範囲であれば、認証する。

【００６９】ステップ１３において、今回の写像変換プログラムProProj $_n$ を用い、AKI_0の写像$AKI_{0,n}^{-1}$を計算する。これは、次回の認証の登録データとするものである。ここで、AKI_0は、Aki $_n$ の値を反映して修正（更新）してもよい。この場合AKI_0はAKI_1とする。ステップ１４において、$AKI_{0,n}^{-1}$を公開鍵暗号方式でサイトA に伝送し、サイトA では、n をn-1 として、$AKI_{0,n-1}^{-1}$として蓄積する。

【００７０】利用者UAの本人認証ができた段階で、同図(30)において、コンテンツを公開鍵暗号方式で伝送する。続いて、第３の実施例について説明する。第３の実施例においては、認証登録データAKI_0をサイトA でもサイトB でも持たない。写像変換された$AKI_{0,n}^{-1}$をサイトB で保管し、その写像変換の解読プログラムをサイトAが保有し、認証の度に写像変換解読プログラムをサイトA からサイトB に伝送し、そのプログラムで写像変換を解読してAKI_0を取り出し、Aki$_n$ と比較する。

【００７１】次に、第３の実施例における利用者登録処理について図９を用いて説明する。以下、図５、図７と異なる部分のみ説明する。ステップ０－２において、バイオ証明証発行要求があると、サイトB において、ProFow、SXPro $_n$ 、SXPro $_n^{-1}$、および、認証データ生成プログラム(秘密)ProLat 、写像プログラムセットを生成するプログラムProSET、認証データ比較プログラムProComを生成する。

【００７２】ProSETは、図７で説明した、ProProj 、ProProj $^{-1}$のセットを生成する。ステップ５０において、ProSETを用いて、今回の写像変換プログラムProProj $_n$ 、次回の写像解読プログラムProProj $_n^{-1}$を生成する。ステップ８－１において、公開鍵暗号方式を用いて、$Kaz_{0,n}^{-1}$、および、ProProj $_n$ を伝送する。

【００７３】ステップ１１において、ProProj $_n$ を用い、AKI_0の写像$AKI_{0,n}^{-1}$を計算し、ステップ１２において、n をn-1 として、$AKI_{0,n-1}^{-1}$をサイトB において登録保管する。次に、図１０を用いて第３の実施例における通信中の処理を説明する。ステップ５０において、ProSETを用いて、ProProj $_n$ 、ProProj $_n^{-1}$を生成する。また、ステップ５１において、前回生成されメモリに蓄積されている「今回使用する写像解読プログラムProProj $_{n-1}^{-1}$」を読み出す。

【００７４】ステップ１１において、前回の写像解読プログラムProProj $_{n-1}^{-1}$を用いて、保管してあるAKI $_{0,n-1}^{-1}$を解読し、AKI_0を計算する。ステップ１２において、ProComn を用い、Aki $_n$ とAKI_0を比較し、Aki $_n$ がAKI_0の許容範囲であれば、認証する。ステップ１３において、今回の写像変換プログラムProProj $_n$ を用い、AKI_0の写像$AKI_{0,n}^{-1}$を計算する。

【００７５】ステップ１４において、n をn-1 として、$AKI_{0,n-1}^{-1}$を登録する。ステップ１５、１６によって、サイトA は、$AKI_{0,n-1}^{-1}$が、サイトB に登録されたことを知る。ステップ５１では、n をn-1 として、ProProj $_{n-1}^{-1}$を保管する。以上の説明において、サイトA とサイトB との通信について説明した。

【００７６】しかし、本発明は、サイトA とサイトB からなる構成に限定されず、例えば、サイトA とサイトBとの間に第３の局（認証局）を設けてもよい。即ち、サービス提供にあたって、利用者はサイトC （認証局）に本人登録（証明証発行要求）を行う。サイトC からサイトA の利用者UAに対して、上記の各実施例においてサイトB からサイトA に伝送されたと同様なプログラム、例えば、ProFow、SXPro などが伝送される。

【００７７】また、サイトC からサイトB に対しては、サイトB で生成していたと同様なプログラム、例えば、ProLat、SXPro $^{-1}$、ProCom等が伝送される。その後の処理は、各実施例でサイトA とサイトB との間で行われた流れでも良いし、また、AKI の計算、保管をサイトC で行っても良い。サイトC （認証局）を信頼性の高い中立的な機関とすることで、個人の特徴情報の管理に関して、より安全なシステムを構築できる。

【００７８】さて、次に、従来の技術で説明したような種々の脅威に対する本発明の安全性について説明する。

（１）まず、本発明における通信中の脅威に対する安全性について説明する。上述したように、本発明では、サイトA,B 間で、認証処理を行う各種プログラム、Kaz 、AKI 等を伝送する。伝送中にデータが盗取される脅威については、公開鍵暗号方式を組み合わせて使用することで対処できる。

【００７９】例えば、サイトB が、前処理過程プログラムProFowをサイトA に確実に伝送しようとするときは、サイトB はサイトA の公開鍵Sk(siteA) で暗号化してサイトA に伝送する。サイトA では、自分の秘密鍵Sk(siteA) でこれを解読し、ProFowを入手する。また、Kaz をサイトA からサイトB に伝送しようとする場合、サイトA では秘密鍵Sk(siteA) で暗号化して伝送し、サイトBでは公開鍵Sk(siteA) で解読してこれを入手する。これにより、サイトB はKaz が確実にサイトA から送られてきたことを知ることが出来る。

【００８０】（２）本発明における利用者とサイトA の間の脅威に対する安全性については、パスワードと指紋を併用する認証方式の場合、パスワードが仮に盗まれた場合でも指紋の認証が出来なければサイトB は利用者を認証することはないので、脅威は少ない。

（３）次に、サイトA 端末内のProFowが解読される場合の脅威に対する安全性について説明する。

【００８１】ProFowが解読されコピーされると、疑似端末を作ってこれに指紋センサを接続することで、Kaz の一つである陵線ベクトルが計算できる環境ができあが

る。しかし、利用者以外が指をセンサに押し当てても、計算されるKaz は正規の利用者とは異なるので、仮にこのKaz がサイトB に伝送されてもAki は異なるので認証はできない。

【００８２】（４）また、正規の利用者センサに指を押した際のKaz を何らかの方法でProFowの中から読みとり、これをサイトB に伝送することにより成りすましが成立するのではないかと言う脅威については、サイトBにおいて、Kaz の揺らぎを検出、または、Kaz を入力とし計算されるAki の揺らぎを検出することで、不審を検出できる。

【００８３】つまり、前述のように、正規な利用者UAがセンサに指を押し当てたときは、Kaz 、あるいは、Aki は所定の揺らぎを持つ。数100 次元のKaz が全く同じ数値で入力されることは確率的に少ない。従って、Kaz やAki の数値を前回と比較し「異常に高い同一性」を認めた場合には、成りすましの脅威を感知して、後述のように回避処理をとることが出来る。

【００８４】（５）Kaz 盗取、偽造の脅威に対抗する手段として、前述したように、本発明においては、Kaz の計算において、これにスクランブルを掛けることを可能としている。それにはプログラムSXPro とこれを解読するプログラムSXPro $^{-1}$ を用いる。前述したように、サイトB は利用者を認証しようとしたときに、SXPro とSXPro $^{-1}$ のセットを用意し、SXPro をサイトA に伝送する。サイトA ではProFowとSXPro をリンクして新しい特徴要素抽出のための前工程プログラムnewProFow を生成する。同プログラムは、認証要求がある毎に変化する。

【００８５】同様に、サイトB では、SXPro $^{-1}$ とProLatをリンクして、新しい後工程プログラムnewProLat を生成する。newProLat は、スクランブルが掛かったKaz を入力として、Aki 、もしくは、AKI を計算する。newProFow は、（１）ProFowを作動させてその出力であるKazにスクランブルが掛かるように作用する構成と、（２）ProFowの処理過程でKaz が計算される途中にKaz の順列にスクランブルが掛かるように作用する構成とが可能である。

【００８６】前者の構成では、二つのプログラムのリンクは簡単であるが、スクランブルの方法が解読されやすい問題がある。後者は、スクランブルのアルゴリズムが完全に解読されない限りKaz を偽造することは難しい。スクランブルのプログラムの半分はサイトB が持つことになるので、（２）の構成を採用することによって、サイトA でのKaz 偽造の脅威は回避できる。

【００８７】次に、サイトB での脅威について説明する。サービスを提供するサイトB 側においても、システム管理者、従業員等による成りすましに不正行為の脅威がある。成りすましは、Kaz の取得と偽造もしくは、AKI の取得とAki 偽造によって可能性がある。このうち、Kaz の取得については、スクランブルが掛かる前述のnewProLat を用いることにより、Kaz がそのまま同プログラムの入力データとなることは無いので、Kaz を簡単に読みとることは困難である。

【００８８】問題は、newProLat の出力である認証データAki 、あるいは、被照合データであるバイオ認証登録データAKI を盗取される脅威である。AKI が盗取されれば、同様な認証データAki を偽造し、両者をProCOMに入力すれば、認証が成立してしまうからである。従って、利用者の中には、AKI をサービス提供側に置くことに対して抵抗感を持つ人もいる。

【００８９】（６）　この対策としては、認証登録データAKI の管理をサイトB ではなく、安全性を確保した上でサイトA で行う方法がある、この詳細については前述した通りである。

（７）　AKI 盗取の脅威を回避する他の手段として、AKI をサイトB で保管するものの、AKI を写像変換し（鍵を用いて一種の暗号を掛ける）、その逆写像変換の鍵をサイトA で保管する本発明の方法が有効である。

【００９０】（８）　次に、成りすまし等の脅威を感知した場合の回避手段について説明する。サービス提供側である、サイトB は、Kaz やAKI を管理し得る環境にあるため、この揺らぎ等を検出して成りすましを推定することが可能である。本発明では、サイトA に伝送したプログラムを利用して認証の前処理を行うので、このプログラムを入れ換えることで脅威に対抗できる。プログラムの入れ換えは、JAVA等を利用し利用者に負担を掛けずにできる。

【００９１】また、あるセンサ（例えば指紋）による認証で成りすまし等の脅威が発覚した場合には、GUI を用いて、利用者に他のセンサから他の人体情報を入力するように指示することができる。他のセンサとしては、筆跡、音声、顔画像、眼の虹彩などが可能である。その中の一例として筆跡の例を図１１（ａ）～（ｄ）に示す。

【００９２】図１１（ａ）は、筆跡入力タブレット出力の例を示す図であり、X 軸、Y 軸、および、筆圧(P軸)が出力される。図１１（ｂ）～（ｄ）は、横軸に時間t 、縦軸にY 軸、X 軸、筆圧(P軸) を取った場合の出力を示す。出力は、1500バイト程度の情報であり、筆跡特徴は、タブレット上のスタート位置、文字の大きさ、スピードによって変化するため、認証データとするためには、位置、文字の大きさ、および、時間の正規化が必要である。

【００９３】位置、文字の大きさは、X 軸、Y 軸の値に対応するので最大最小値の幅を合わせることによって正規化する。時間はスタートから終了までの時間が一定になるように正規化する。正規化が済んだデータは、予め、同一利用者から同様にして取得した認証登録データと比較する。

【００９４】図１２は、比較の例である。図１２（ｃ）における実線が認証登録データAKI 、破線が認証データ

Aki である。両者の比較には、例えばDPマッチング処理が可能である。同図の四角枠の拡大図に示すように、２つの線のサンプル点間の距離を対応する候補点を順次移動させながら求め、該距離の和が最小になるところで収束させる。その結果としては、２本の線の隙間を表すパラメータが得られる。Y 軸、X軸、筆圧(P軸) について同様な処理を行い、各軸の誤差の和を求める。

【００９５】なお、誤差の出現の仕方が各軸で異なるので、個体間の差が大きな軸に対して重みを付けることが可能である。具体的には、成りすましの脅威を考えた場合、文字の形、即ち、Y 軸、X 軸の出力については偽造しやすいが、圧力P については隠れた特徴なので偽造が難しい。従って、P 軸の特徴に重みを付けて認証しても良い。

【００９６】このようにして得られた誤差の和が、所定のしきい値以下にあれば本人として照合する。本発明に筆跡を適用する場合、プログラムの前工程、後工程の分割は様々可能であるが、例えば、ProFowの処理として、Y 軸、X 軸、筆圧(P軸) の信号列 (Kaz) を取り出すところまでとし、ProLat、ProCOMの処理として、正規化、DPマッチング処理、誤差合計処理、しきい値処理などとすることが可能である。

【００９７】また、正規化の処理までを前工程とし、DPマッチング、各軸の誤差合計処理、しきい値処理を後工程とすることも可能である。以上のように、複数のバイオセンサを利用することが可能であり、この場合、ProLatの統合処理が重要になるが、様々な統合方法が可能である。例えば、（１）様々な特徴要素Kaz を各次元とする多次元空間で認証登録データAKI と認証データAki との間の距離を計算し、所定のしきい値以内であれば認証成立とする方法。具体的には、例えば、指紋の隆線ベクトルm 次元と筆跡のX 軸足＋Y 軸＋P 軸のn 次元を組み合わせ、m+n 次元で認証する方法、（２）各センサから得られる類似度（登録認証データと認証データとの差分）を各々求め、そのデータの確からしさを重として掛け合わせ、しきい値処理する方法、等が可能である。

【００９８】上述した各構成要素を実現するプログラムはＣＤ－ＲＯＭやフロッピーディスク等の記録媒体に格納することができる。記録媒体に格納されたプログラムをコンピュータにインストールすることにより本発明の各処理装置の処理を行うことが可能である。また、上記のプログラムをコンピュータにプレインストールしておくことも可能である。

【００９９】なお、本発明は上記の実施例に限定されることなく、特許請求の範囲内で種々変更・応用が可能である。

【０１００】

【発明の効果】本発明によれば下記に示す種々の効果を得ることが可能である。

（１）セキュリティホールが少なく、高い安全性

個人の身体的特徴を用いる個人認証方法において、本発明の特徴は、認証処理の全てを、例えば、バイオセンサ、サイトA 、サイトB 等のどこか１カ所で行うのではない。すなわち、個人特徴抽出のプログラムを複数に分割して、サイトAでは前工程プログラムを保有し、これを起動して利用者の特徴要素を抽出する。その特徴要素は、サイトB に送信される。サイトB では後工程プログラムを保有し、該特徴要素の数値変換、正規化、参照特徴とのマッチング処理などを行う。

【０１０１】本発明では、このように、認証処理の分割や認証データの管理を工夫しているため、利用者とバイオセンサ、バイオセンサとサイトA 、サイトA とサイトB 、サイトB とサイトB 管理者のどの部分にも、セキュリティホールが存在しないような構成とすることが可能である。従って、どこか１カ所がアタックされると簡単にアルゴリズムが解読されると言う脅威が少ない。

【０１０２】このように、従来指摘されるセキュリティホール問題の多くを解決できる効果がある。

（２）サービス内容と整合性の取れた認証処理を実現できる

認証処理の前工程、後工程の一連のプログラムをサイトB 側で用意することができるので、サイトB は、アルゴリズムを自ら評価、または、認証局のような公的第３者機関によって評価してもらい、自分が納得した上で、その一部をサイトA に提供できる。サービスする側に取っては、サービスに適した認証精度のアルゴリズムを選択できる効果がある。

【０１０３】

（３）認証方式の更新、および、メンテナンスが容易

サイトA 側には、前処理工程のプログラムがサイトB から送信されるため、サイトA 側で第３者による解読の脅威等があった場合には、そのプログラムを直ぐに更新できるため、脅威を速やかに排除できる効果がある。

（４）認証の利便性が向上

サイトA には、センサが接続されるが、そのセンサの生データを処理して利用者特徴要素を計算する前工程プログラムはサイトB から送信される。

【０１０４】従って、利用者は、様々なセンサを自らの判断でサイトA に接続して、その前工程プログラムをサービス提供側から送ってもらうことができる。また、サイトB は、新サービスを開始するに当たって、バイオセンサをサイトA に接続し、その前工程プログラムを伝送して利用可能にすることができる。つまり、各種バイオセンサを拡張することは簡単に可能である。利用できるバイオセンサが増えれば、組み合わせを選択することが可能になる。

【０１０５】例えば、パスワードを覚え難い、高齢者、痴呆等の要介護者、子供などには、パスワードの変わりに、指紋で代用することが可能である。更に、指紋に心理的抵抗感のある人に対しては、所望の認証精度を確保

27

すると言う前提のもとで、例えば、顔画像、音声、筆跡、眼の虹彩画像、パスワード、等を組み合わせることが可能である。

【０１０６】更に、サービス提供側からしても、例えば、現在パスワード４桁でサービスを実施中であって、利用者が更にリスクの大きなサービス（具体的には、高額の現金引き出しサービス）を要求しているような場合で、パスワードの桁を増やすことがサービス低下になると考えられるような場合には、パスワード４桁に加えて、指紋認証を行うことが可能である。仮に、指紋認証で４桁の精度が得られれば、２つを組み合わせることで、８桁の認証精度が実現され、サービス側は安心してそのサービスを提供できると言う効果がある。

【０１０７】（５）通信コストが安い

利用者とサービス側との間で伝送される情報は、個人特徴要素Kaz とこれをスクランブルする手段、認証登録データAKI とこれを写像変換する手段である。人体情報の生データをそのまま送る場合に比較し、通信に掛かるコストは低い。

（６）犯罪の予防効果

サービス提供側、または、サービス提供側の意向による認証代行側（認証局側）では、個人特徴要素Kaz 、認証データAki などを知り得る状況にある。バイオメトリックス情報の特徴は、揺らぎがあることである。例えば、指紋であれば、センサに指を当てる力、タイミングなどによって、同一人であってもわずかに変化する。この揺らぎは、Kaz やAki に反映されるため、これを検出するサービス提供側では、この揺らぎを把握することができる。

【０１０８】バイオメトリックスで認証をする際、成りすましによる不正の脅威として、指紋を写真に取ってセンサに近づけるなどが考えられる。この場合、生体が直接センサに触れないので、揺らぎが生じない、または、揺らぎが生体の場合と異なる。従って、この揺らぎを検出することによって、成りすましによる利用を推定できる。成りすまし等の不審が発見された場合、指紋から筆跡や音声など、他のバイオメトリックスに変えるなどの対策が可能であり、安全性が高い。

【０１０９】また、不審者を推定した場合、顔画像を用

28

いるとか、音声を用いる等に切り替えることにより、犯罪の予防効果が期待できる。つまり、顔画像や音声情報が利用されることになると、不審者にとっては、犯罪捜査が自分に及びやすくなる訳で、犯罪に対するリスクがあるため、成りすましを避ける効果があると考えられる。

【図面の簡単な説明】

【図１】本発明における個人認証システムの基本構成を示す図である。

【図２】指紋の特徴要素が隆線ベクトルの場合の抽出例を示す図である。

【図３】隆線ベクトルの例を示す図である。

【図４】２本の指紋隆線の和を求めた概念を示す図である。

【図５】第１の実施例における利用者登録処理を示す図である。

【図６】第１の実施例における通信中の処理を示す図である。

【図７】第２の実施例における利用者登録処理を示す図である。

【図８】第２の実施例における通信中の処理を示す図である。

【図9 】第３の実施例における利用者登録処理を示す図である。

【図１０】第３の実施例における通信中の処理を示す図である。

【図１１】人体情報として筆跡を用いた場合を説明するための図である。

【図１２】人体情報として筆跡を用いた場合の比較方法を説明するための図である。

【図１３】従来技術における公開鍵暗号方式を説明するための図である。

【図１４】従来技術における公開鍵暗号方式を説明するための図である。

【符号の説明】

１、７　処理装置

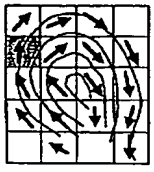
３　モニタ

５、９　通信手段

１１　ネットワーク

【図２】

指紋の特徴要素が隆線ベクトルの場合の抽出例を示す図

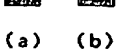


【図３】

隆線ベクトルの例を示す図

【図４】

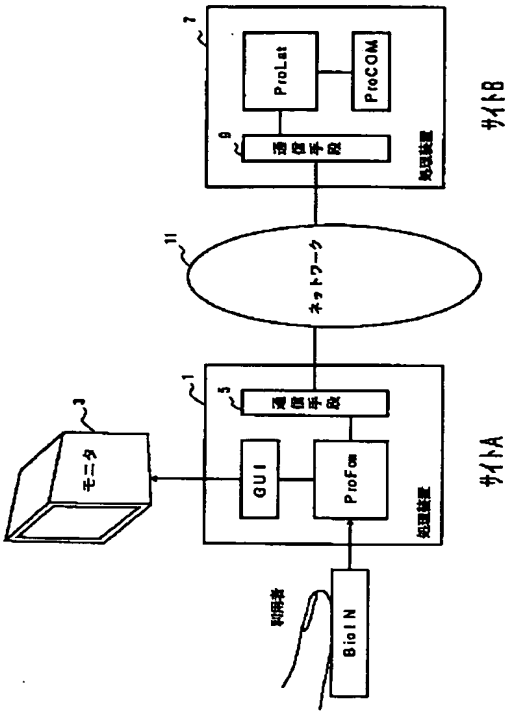
２本の指紋隆線の和を求めた概念を示す図



(a)　(b)

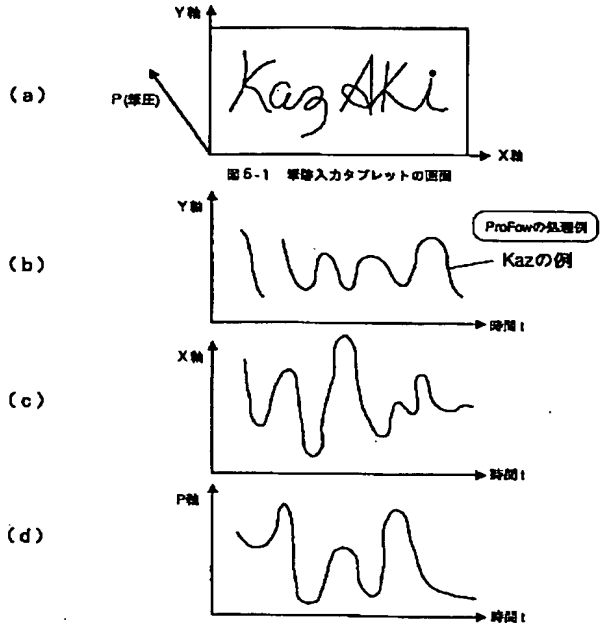
【図１】

本発明における個人認証システムの基本構成を示す図



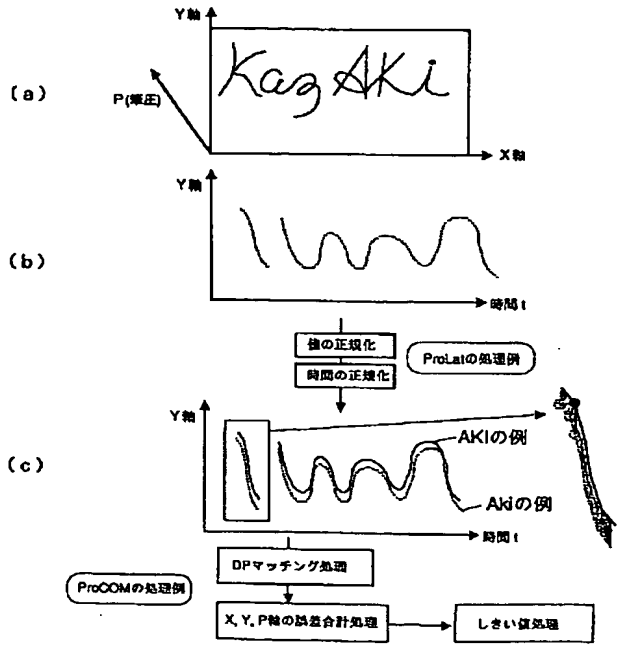
【図１１】

人体情報として筆跡を用いた場合を説明するための図



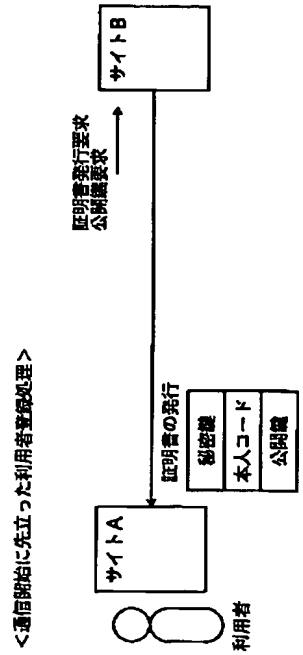
【図１２】

人体情報として筆跡を用いた場合の
比較方法を説明するための図



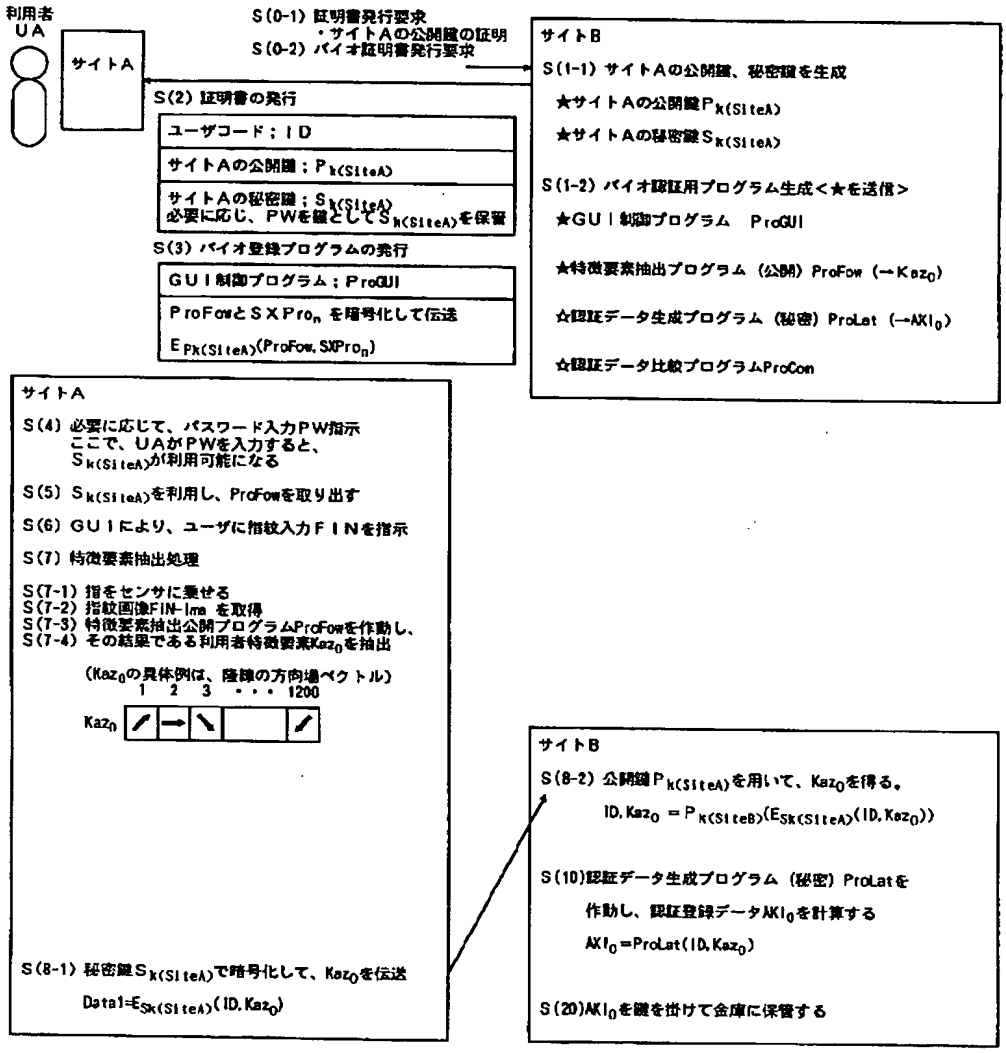
【図１３】

従来技術における公開鍵暗号方式を説明するための図



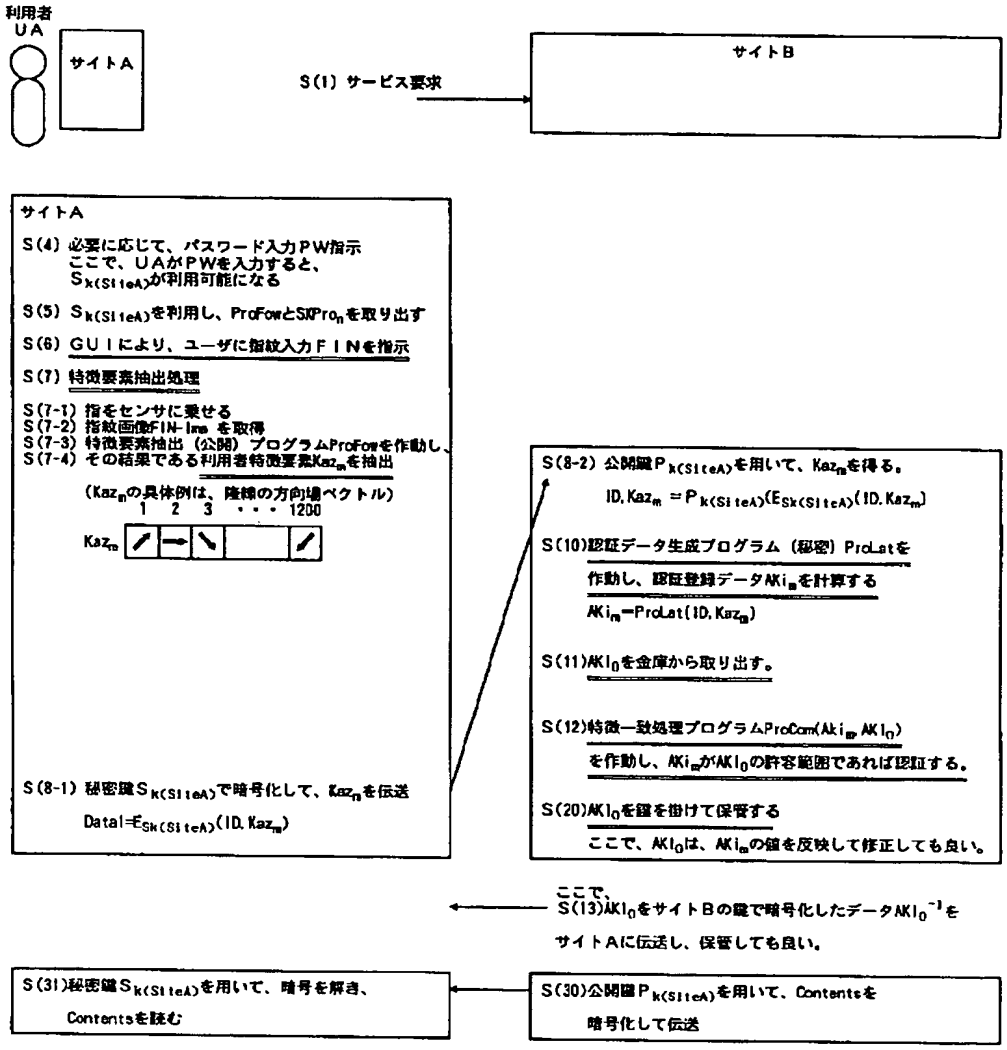
【図５】

第１の実施例における利用者登録処理を示す図



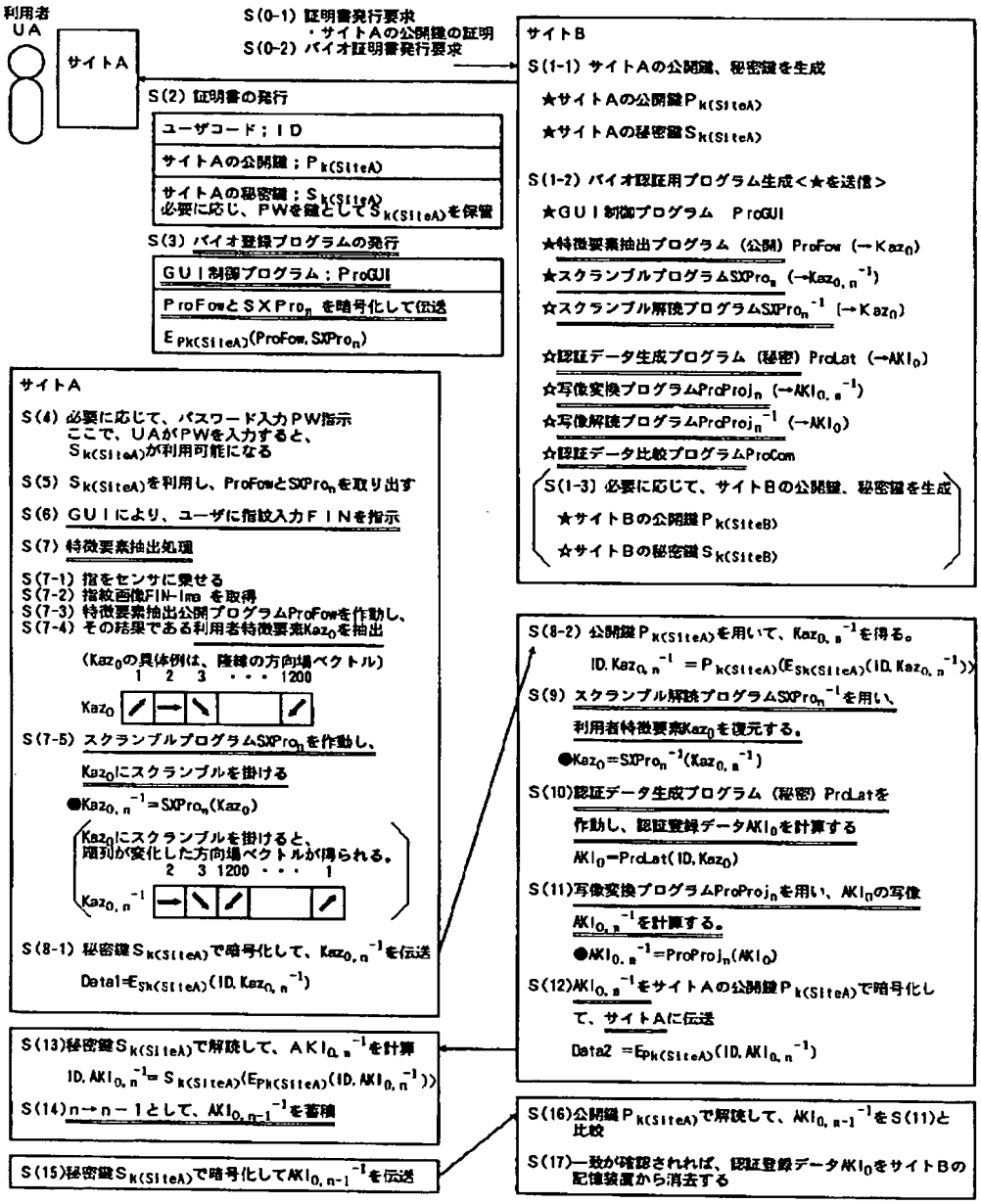
【図６】

第１の実施例における通信中の処理を示す図



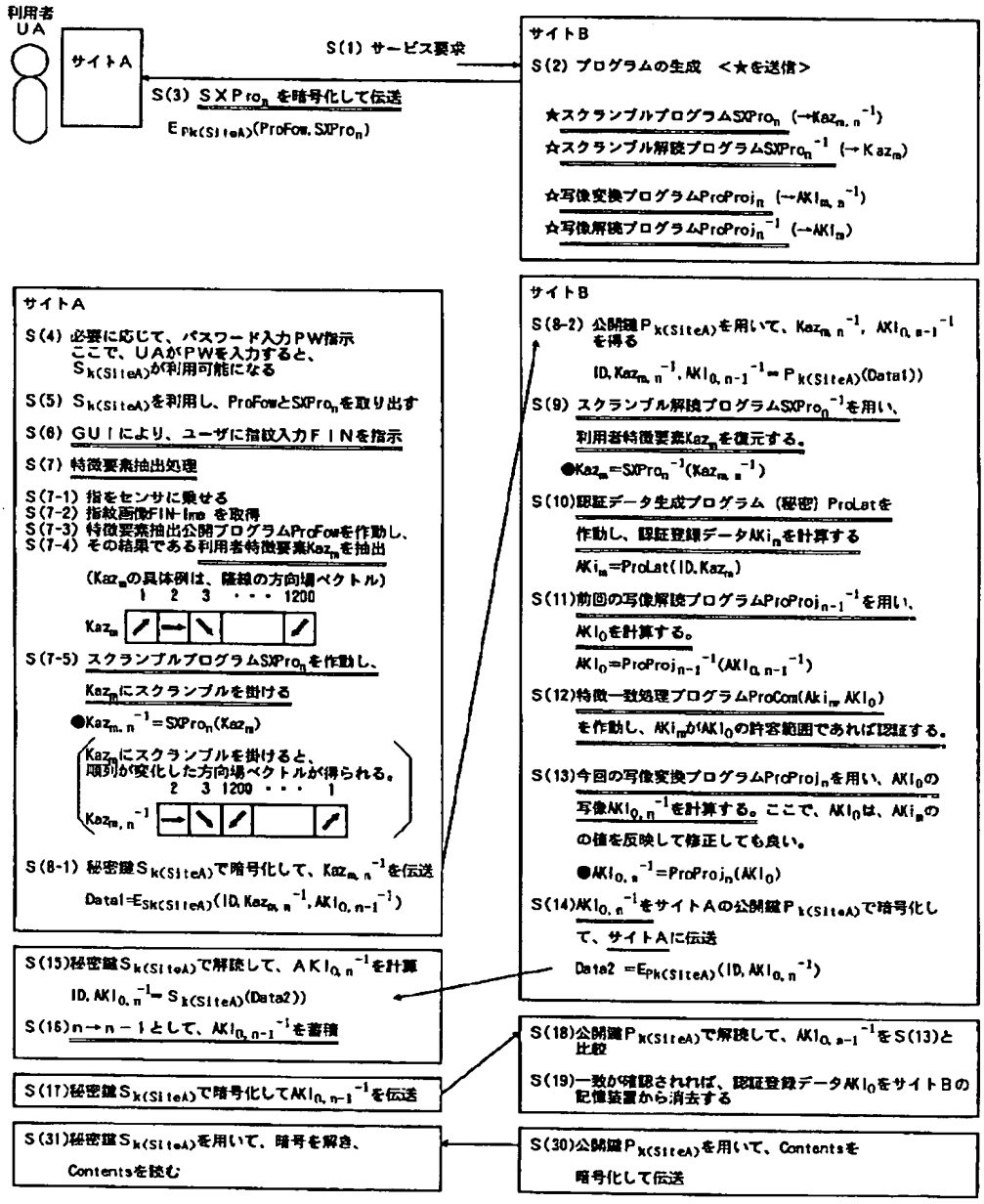
【図７】

第２の実施例における利用者登録処理を示す図



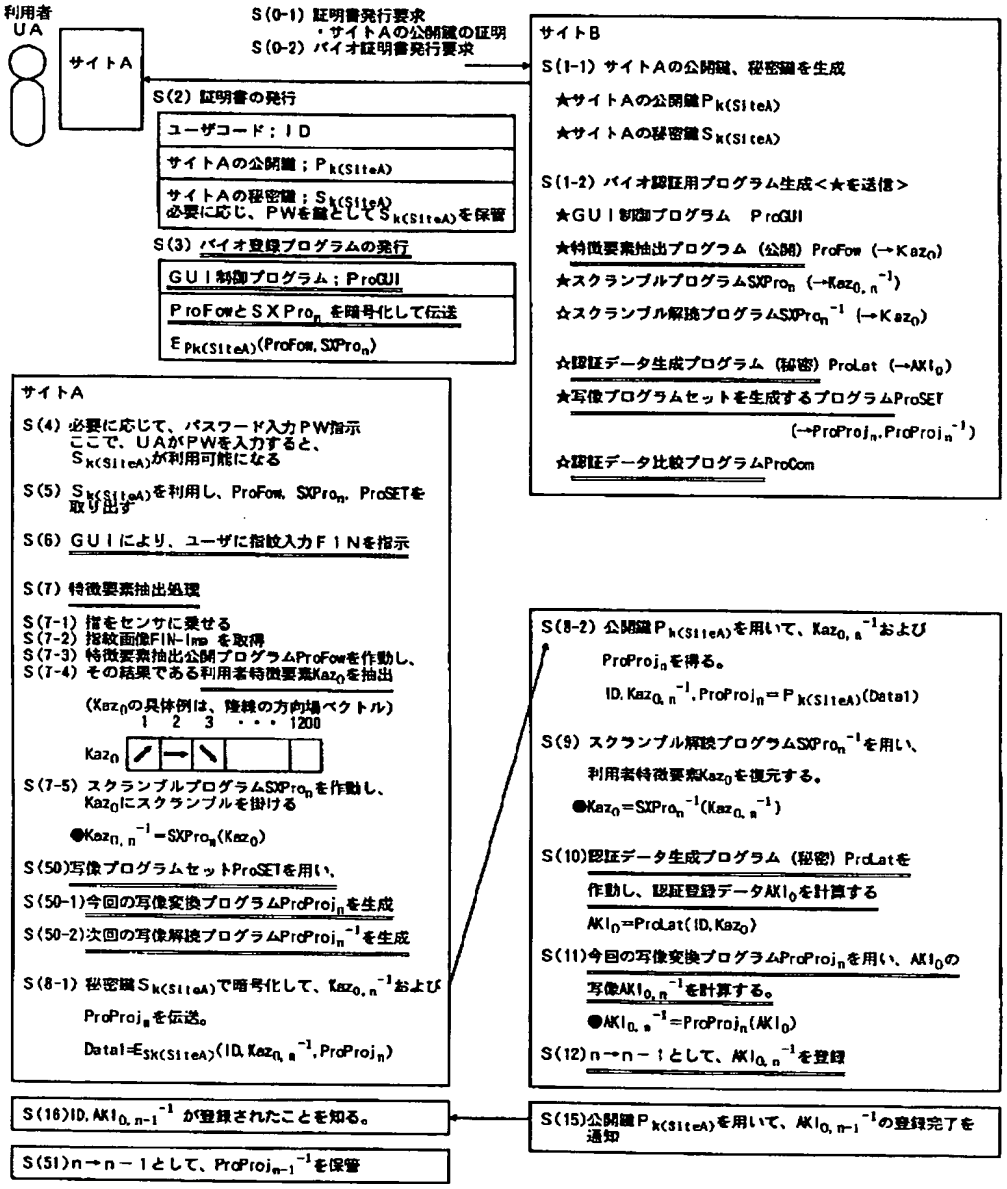
【図８】

第２の実施例における通信中の処理を示す図



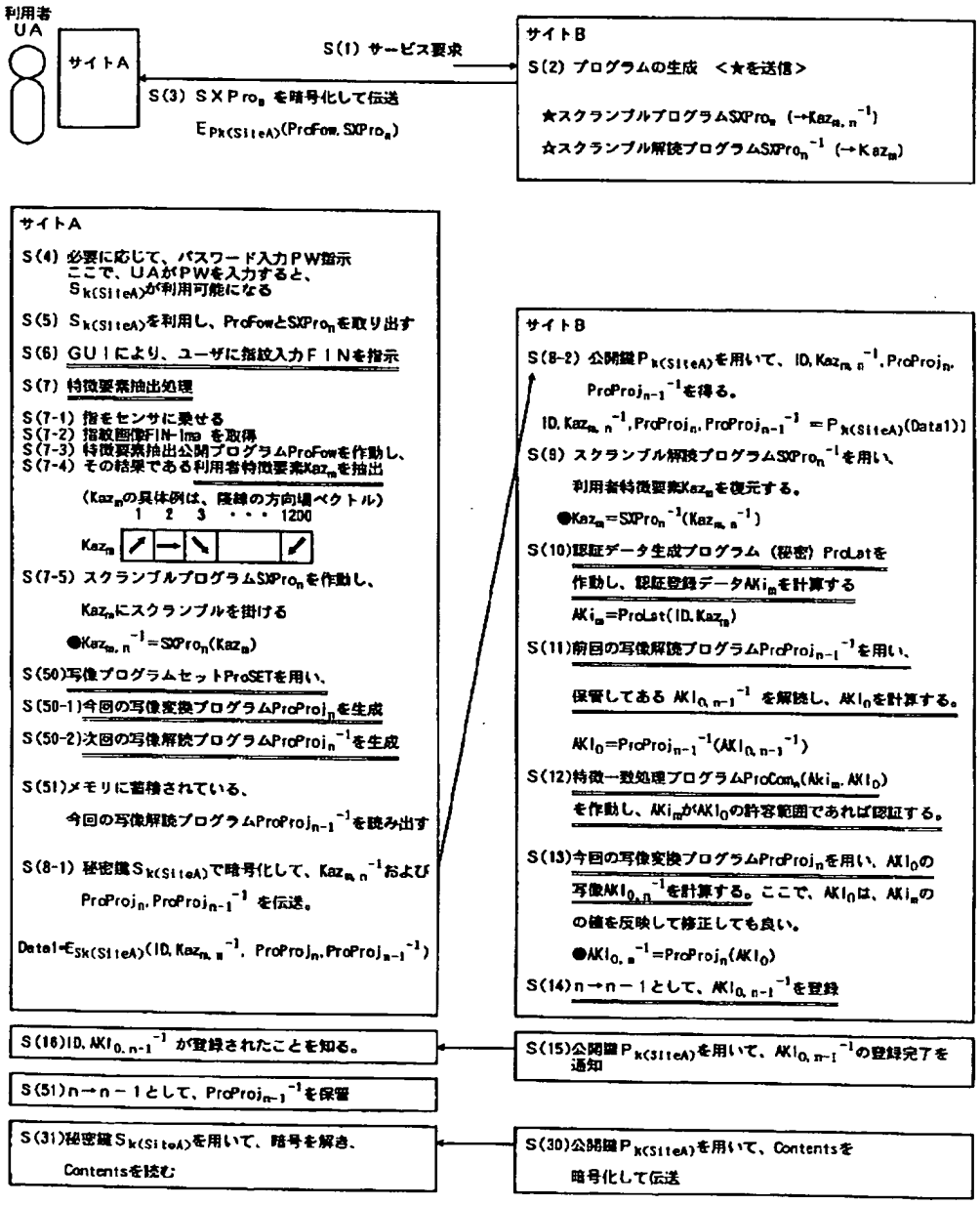
【図９】

第３の実施例における利用者登録処理を示す図



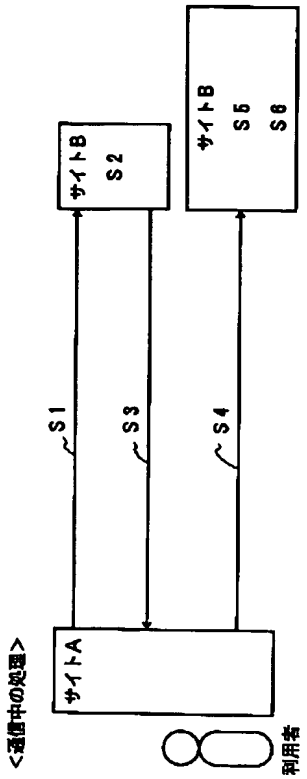
【図１０】

第３の実施例における通信中の処理を示す図



【図１４】

従来技術における公開鍵暗号方式を説明するための図



フロントページの続き

(72)発明者　若原　徹
東京都千代田区大手町二丁目３番１号　日本電信電話株式会社内
(72)発明者　外波　雅史
東京都千代田区大手町二丁目３番１号　日本電信電話株式会社内
(72)発明者　堀岡　力
東京都千代田区大手町二丁目３番１号　日本電信電話株式会社内
(72)発明者　山中　喜義
東京都千代田区大手町二丁目３番１号　日本電信電話株式会社内
(72)発明者　田中　清人
東京都千代田区大手町二丁目３番１号　日本電信電話株式会社内
(72)発明者　小松　尚久
東京都国分寺市光町１－26－24
Ｆターム(参考)　5B043 AA09 BA01 BA02 BA05 BA06
CA09 FA02 FA07 GA17
5B085 AE23 AE25 AE26 AE29